TU WIEN Informatics

Structured Development of Organisational Cyber-Resilience

DIPLOMA THESIS

submitted in partial fulfillment of the requirements for the degree of

Diplom-Ingenieur

in

Business Informatics

by

Jonathan Denzel, B.Sc.
Registration Number 12127086

to the Faculty of Informatics

at the TU Wien

Advisor: Ao. Univ.-Prof. Mag. Dr. iur. Markus Haslinger

Vienna, October 7, 2024

Jonathan Denzel	Markus Haslinger

Technische Universität Wien
A-1040 Wien ▪ Karlsplatz 13 ▪ Tel. +43-1-58801-0 ▪ www.tuwien.at

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

TU WIEN Informatics

Strukturierter Aufbau organisatorischer Cyber-Resilienz

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Wirtschaftsinformatik

eingereicht von

Jonathan Denzel, B.Sc.
Matrikelnummer 12127086

an der Fakultät für Informatik

der Technischen Universität Wien

Betreuung: Ao. Univ.-Prof. Mag. Dr. iur. Markus Haslinger

Wien, 7. Oktober 2024

Jonathan Denzel	Markus Haslinger

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

TU Bibliothek Your knowledge hub

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Erklärung zur Verfassung der Arbeit

Jonathan Denzel, B.Sc.

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 7. Oktober 2024

Jonathan Denzel

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Danksagung

Bevor ich den letzten Punkt meiner Masterarbeit setze, möchte ich die Gelegenheit nutzen, um all jenen zu danken, ohne deren Unterstützung, Ermutigung und Beiträge diese Arbeit nicht möglich gewesen wäre.

Zunächst gebührt mein tiefster Dank meinen Eltern. Nicht nur durch eure unerschütterliche Liebe und tatkräftige Unterstützung, sondern auch eure Geduld und euer Verständnis sind mir eine unverzichtbare Stütze im Leben.

Meinen Freunden möchte ich ebenso herzlich danken. Ihr seid mein Fels in der Brandung. Euer offenes Ohr für meine Sorgen und eure Bereitschaft mir mit Rat und gelegentlich notwendiger Ablenkung zur Seite zu stehen haben mich durch diese Arbeit getragen.

Meinem Vorgesetzten und meinen Kollegen von Certitude Consulting möchte ich danken, dafür dass ihr mir die Türen geöffnet habt, um wertvolle thematische Einblicke und Interviews mit Fachexperten zu gewinnen. In diesem Zuge möchte ich mich auch bei der OeNB, insbesondere bei Herrn Unteregger, bedanken für die Bereitschaft mit mir zu sprechen.

Ein besonderer Dank gebührt meinem Betreuer, dessen Expertise, zeitliche Flexibilität und Zuversicht entscheidend für meinen Erfolg waren.

Besonders hervorheben möchte ich euch: Eileen, Ylva, Helena, Caren und Konstantin. Ihr habt euch die Zeit genommen, Entwürfe zu lesen, Transkripte zu schreiben und Feedback zu geben. Eure konstruktiven Kommentare und Anregungen waren von großem Wert und haben wesentlich dazu beigetragen, die Klarheit und Qualität meiner Arbeit zu verbessern.

Zum Schluss möchte ich jedem, der mich auf dieser Reise begleitet hat, meinen tiefsten Dank aussprechen. Diese Arbeit ist nicht nur das Ergebnis meiner eigenen Bemühungen, sondern auch das Produkt der vielen Menschen, die mich auf meinem Weg unterstützt haben.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Abstract

The prevalence and damage caused by cyber-attacks on companies worldwide have grown significantly over the last few decades, posing the greatest threat to Information and Communication Technology (ICT) in today's digital service world.

European organisations in critical sectors are subject to regulation regarding cybersecurity. Laws, including the Digital Operational Resilience Act (DORA), the Network and Information Security Directive (NIS2), and the European Banking Authority (EBA) guidelines, are put in place to regulate the robustness of cybersecurity within corresponding organisations. Organisational frameworks such as the ISO2700X and ITIL4 generally guide cyber-resilience efforts.

In this master thesis, a project plan template for financial institutions is constructed and evaluated to develop organisational cyber-resilience and reduce the risk of cyber threats and legal penalties under DORA. The project plan template is structured around common organisational frameworks and regulations, providing a basis for financial institutions to coordinate their DORA-related cyber-resilience efforts.

The context of this cyber-resilience project plan template is further explored through an interview with Austria's lead implementer for DORA audits and contributor to DORA at the Austrian National Bank (OeNB) and an in-depth analysis of the facets of resilience.

This thesis employs the design science research framework, which includes literature research, requirements engineering, artefact creation, and qualitative evaluation through analytical verification and expert interviews. Design science facilitates the practical application of the findings in real-world settings, demonstrating the relevance and applicability of this work to the field and thereby contributing to the broader field of information security management.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Kurzfassung

Die Häufigkeit und der Schaden, den Cyberangriffe auf Unternehmen weltweit verursachen, haben in den letzten Jahrzehnten erheblich zugenommen und stellen die größte Bedrohung für die Informations- und Kommunikationstechnologie (IKT) in der modernen digitalen Service-Welt dar.

Europäische Organisationen in kritischen Sektoren unterliegen der Regulierung im Bereich der Cybersicherheit. Rechtsvorschriften wie der Digital Operational Resilience Act (DORA), die Network and Information Security Directive (NIS2) und die Richtlinien der Europäischen Bankenaufsichtsbehörde (EBA) regeln die Cybersicherheit in den betreffenden Institutionen. Organisatorische Rahmenwerke wie ISO2700X und ITIL4 dienen als Leitfaden für die Entwicklung von Cyber-Resilienz.

In dieser Masterarbeit wird eine Projektplanvorlage für Finanzinstitute erstellt und bewertet, um die organisatorische Cyberresilienz zu entwickeln und das Risiko von Cyberbedrohungen und rechtlichen Sanktionen im Rahmen von DORA zu verringern. Die Projektplanvorlage ist auf der Grundlage allgemeiner organisatorischer Rahmenbedingungen und Vorschriften aufgebaut und bietet den Finanzinstituten eine Grundlage für die Koordinierung ihrer Cyber-Resilienzbemühungen im Hinblick auf DORA.

Der Kontext dieser Projektplanvorlage für Cyberresilienz wird durch ein Interview mit Österreichs federführendem Umsetzer für DORA-Audits und Mitgestalter der DORA bei der Österreichischen Nationalbank (OeNB) sowie durch eine eingehende Analyse der unterschiedlichen Facetten von Resilienz näher beleuchtet.

Diese Arbeit verwendet den “Design Science”-Forschungsrahmen, der Literaturrecherche, Requirements Engineering, Artefakterstellung und qualitative Evaluierung durch analytische Überprüfung und Experteninterviews umfasst. Design Science erleichtert die praktische Anwendung der Ergebnisse in realen Umgebungen, zeigt die Relevanz und Anwendbarkeit der Arbeit im Feld und trägt so zum allgemeinen Bereich des Informationssicherheitsmanagements bei.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Abkürzungen

AICPA American Institute of Certified Public Accountants

BCM Business Continuity Management

BIA Business Impact Analysis

BSI German Federal Office for Information Security

BWG Bankwesengesetz

CD-RISC Connor-Davidson Resilience Scale

CISO Chief Information Security Officer

COBIT Control Objectives for Information and Related Technologies

COSO Committee of Sponsoring Organizations of the Treadway Commission

CRA Cyber Resilience Act

CSF Cybersecurity Framework

CTO Chief Technology Officer

DLP Data Loss Prevention

DORA Digital Operational Resilience Act

EBA European Banking Authority

ENISA European Network and Information Security Agency

ESA European Supervisory Authorities

EU European Union

FMA Finanzmarktaufsichtsbehörde

GDPR General Data Protection Regulation 2016/679

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

HR Human Ressources

ICT Information and Communication Technology

ISMS Information Security Management System

ISO International Organization for Standardization

ITIL Information Technology Infrastructure Library

ITS Implementing Technical Standards

ITSCM IT Service Continuity Management

KPI Key Performance Indicator

NAC Network Access Control

NIS2 Directive on measures for a high common level of cybersecurity across the Union

NISG Netz- und Informationssystemsicherheitsgesetz

NIST National Institute of Standards and Technology

OeNB Austrian National Bank

PCI DSS Payment Card Industry Data Security Standard

PSD2 Revised Payment Services Directive

RIS Rechtsinformationssystem des Bundes

RPO Return Point Objective

RQ Research Question

RTO Return Time Objective

RTS Regulatory Technical Standards

SABSA Sherwood Applied Business Security Architecture

SIEM Security Information and Event Management

SLA Service Level Agreement

SOC System and Organization Controls

SP Special Publication

TLPT Bankwesengesetz

TOM Technical and Organisational Measures

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

TSC Trust Service Criteria

ZaDiG Zahlungsdienstegesetz

Contents

1 Introduction **1**
- 1.1 Motivation . . . 1
- 1.2 Research Questions . . . 5
- 1.3 Objectives of this master thesis . . . 5
- 1.4 Relevance to the Business Informatics MSC Program at TU Wien . . . 6
- 1.5 Significance of this master thesis . . . 6

2 Applied Research Methods **7**
- 2.1 Design Science Research . . . 7
- 2.2 Literature Review . . . 9
- 2.3 Qualitative Evaluation: Semi-Structured expert interviews . . . 10
- 2.4 Design Verification . . . 12

3 Semi-Systematic Literature Review **13**
- 3.1 Purpose and Scope . . . 13
- 3.2 Conducting the Review . . . 13
- 3.3 Analysis . . . 14
- 3.4 Synthesis and Meta-Narrative . . . 23
- 3.5 Conclusion . . . 25

4 Understanding Systemic Digital Operational Resilience **27**
- 4.1 Resilience in other Disciplines . . . 27
- 4.2 Systemic Resilience . . . 31
- 4.3 Triad of Resilience: Resistance, Maintaining to Operate & Recovery . . . 34
- 4.4 Motivation of the Digital Operational Resilience Act (DORA) . . . 36
- 4.5 Digital Operational Resilience Act (DORA) Audits at the Austrian National Bank . . . 37

5 Development of a Project Plan Template **41**
- 5.1 Requirements Engineering . . . 41
- 5.2 Design and Creation of the Project Plan Template . . . 43

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

6 Design Verification against Requirements **45**
6.1 Legal Verification . . . 45
6.2 Technical Verification . . . 54
6.3 Threats mapping to Working Packages . . . 62

7 Qualitative Evaluation through Expert Interviews **65**
7.1 Selection of Experts . . . 65
7.2 Conducting Expert Interviews . . . 66
7.3 Interview Data Analysis Methods . . . 66
7.4 Results . . . 67

8 Results and Discussion **73**
8.1 Design Verification against Requirements . . . 73
8.2 Findings from the Expert Interviews . . . 75
8.3 Discussion of Results . . . 75

9 Conclusion **77**
9.1 Summary of the Study . . . 77
9.2 Contributions to the Field . . . 77
9.3 Limitations . . . 78
9.4 Future Research Directions . . . 79

A Expert Interview Guideline **81**
A.1 Purpose . . . 81
A.2 Confidentiality . . . 81
A.3 Format . . . 81
A.4 Questions in English . . . 82
A.5 Questions in German . . . 82

B Project Plan Template **85**
B.1 Organisational Governance . . . 89
B.2 IT Controls . . . 98
B.3 Technical Implementation . . . 108

C Transcripts of Expert Interviews **113**
C.1 Interview 1 . . . 113
C.2 Expert Interview 2 . . . 122
C.3 Expert Interview 3 . . . 130

D OeNB Interview on Digital Operational Resilience Act (DORA) **135**
D.1 Purpose . . . 135
D.2 Confidentiality . . . 135
D.3 Format . . . 135
D.4 Prepared Questions in German . . . 136
D.5 Interview Transcription . . . 136

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

CHAPTER 1

Introduction

1.1 Motivation

The damage caused by cyber-attacks to companies all around the globe has grown significantly over the last decades and is the biggest threat to Information and Communication Technology (ICT) in today's world of digital services. Organisations must defend themselves against cyber threats to protect their ICT-related assets, including systems, processes, and sensitive information, thereby working towards the security goals of confidentiality, integrity, availability, and authenticity. Those security goals enable not only the operations and the financial performance but also determine the reputation of organisations.

Moreover, companies operating in systemically relevant sectors within the European Union, such as finance and energy supply, are subject to intense regulation regarding their cyber-resilience. The current legislation, such as the Digital Operational Resilience Act (DORA), Directive on measures for a high common level of cybersecurity across the Union (NIS2), and the European Banking Authority (EBA) guidelines, are put in place to regulate the robustness of the cyber-resilience of the corresponding organisation. This legislation aims to enhance the ability to withstand cyber threats and maintain consumers' trust in critical services.

Resilience from the Latin word **resiliens**, **re** meaning back and **salire** meaning jump, refers to the ability of a system to return to a previous state [Res23c]. In the context of this master thesis, organisational cyber-resilience refers to the following three attributes: The ability to withstand threats to ICT-assets such as attacks, natural disasters, or high demand. Secondly, the capability of an organisation to continue to operate during duress.Thirdly, the quick recovery of ICT-assets from threats, thereby jumping back into a regular state of operation. Cyber-resilience, information security, cybersecurity, and IT-Security are often used interchangeably in the literature.

To build cyber-resilience in organisations, a panoply of international frameworks and standards exists to guide Chief Information Security Officer (CISO)s and Chief Technology Officer (CTO)s in establishing internal controls. For instance, the ISO2700X family offers comprehensive guidelines regarding Information Security Management System (ISMS). Similarly, the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) provides a more risk-based approach to managing cybersecurity risks. The German Federal Office for Information Security (BSI) IT-Grundschutz Compendium entails best practices in securing information assets, and the American System and Organization Controls (SOC) 2 defines Trust Service Criteria (TSC) along which the security of service organisations can be audited and reported.

1.1.1 Cyber Threats to Organisations

With global cyber crimes rising exponentially, the total resulting cyber-attack costs doubled in the last four years, according to the Statista Technology Market Outlook [cyb23]. In 2020, the European Union estimated the global economy's cost of € 5.5 trillion due to cyber crime[EU-22]. The financial sector is especially threatened due to its direct connection to extensive financial gains and the systemic disruption that successful large-scale attacks could cause. The attack surface for organisations is large. The most common threats, according to the European Network and Information Security Agency (ENISA) threat landscape of 2023 [Eni23] (page 8), that organisations face include:

- **Ransomware** refers to a specific attack that encrypts organisations' data through malware, thereby rendering it useless. The goal of a ransomware attack is to demand the payment of a ransom for the promised decryption of files.
- **Malware** refers to malicious code or logic distributed as firmware or general software that runs unauthorised processes and causes damage to an ICT system.
- **Social Engineering** refers to the compromise of individuals with access to ICT assets to perform actions that benefit attackers. The compromise happens through misusing social norms with no or low technical effort.
- **Threats against data** refer mainly to data breaches and data leaks, where sensitive information is published without authorisation or intention of the information owner.
- **Threats against availability: Denial of Service** refers to the (temporary) interruption of the availability of a service. Denial of Service attacks either exhaust the service or the network connecting it to the intended user group.
- **Threats against availability: Internet threats** refers to the inability of services to reach the Internet due to malicious intent or accidents between the service and the Internet. Possible triggers include earthquakes, blackouts, censorship, and cable cuts.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

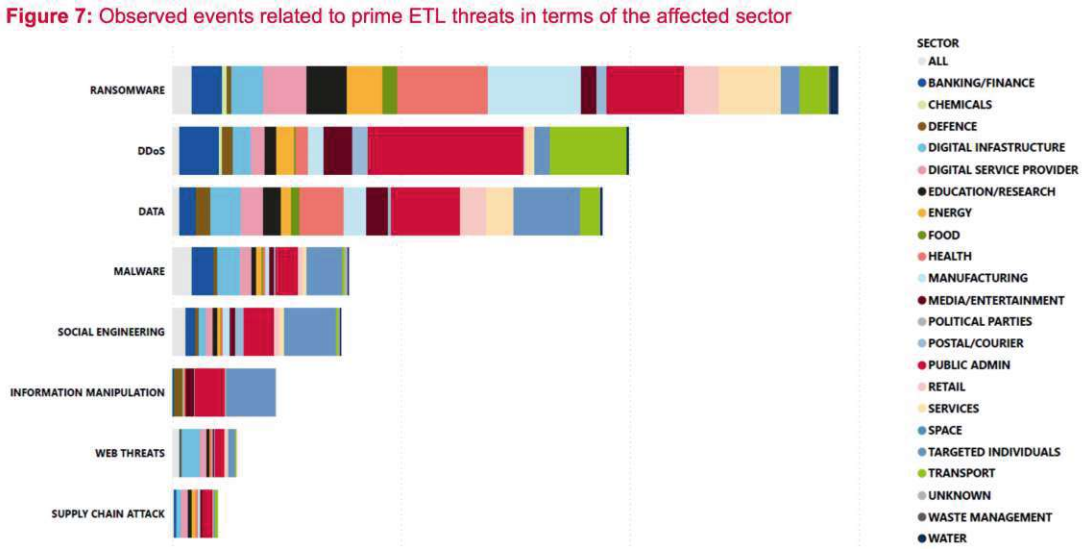


Figure 1.1: Information security events split by sector and threat, as in [Eni23] (page 15)

.

- **Information manipulation and interference** refers to the semi-legal deliberate negative manipulation of values, procedures, and political processes mostly executed by state actors and their proxies in an intentional and coordinated effort.

- **Supply-chain attacks** refers to attacks that target at least two organisations with a supplier-customer relationship through a combination of two distinct attacks. The most famous example of this kind of attack is the SolarWinds attack [Sol21].

Figure 1.1 showcases the most common threats split by actual events per sector. After careful analysis of the figure, it can be inferred that the threat of information manipulation and web threats were less prevalent, and DDOS, Ransomware, Malware, and Data were more prominent threats to the financial sector.

Securing ICT-systems requires the implementation of numerous Technical and Organisational Measures (TOM). Managing that diverse TOM - from a secure hiring process to Business Continuity Management - requires diverse actions and is a nontrivial task.

1.1.2 Legal compliance of financial institutions

Due to the importance of the financial industry for the functioning of the general economy, lawmakers worldwide introduced legislation that ICT-systems of banks and other financial institutions are obliged to comply with. Being aware, understanding, and fully complying with numerous laws and regulations governing the ICT of financial institutes becomes increasingly burdensome as the new legislature is released from state-level institutions such as national banks and international governmental institutions such as the EBA.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

1.1.3 Understanding the industry standards landscape

Compliance with laws often entails compliance with industry standards. Here, the most prominent example in data processing is Article 32 of the General Data Protection Regulation 2016/679 (GDPR), regarding cybersecurity. The law states that appropriate TOM have to be implemented per a risk analysis to ensure, among others, confidentiality, integrity, and availability. While the text itself does not directly refer to industry standards, the recital 78 GDPR mentions the 'state-of-the-art' concerning data protection as appropriate TOM. Further, Article 25 of the NIS2 encourages using European and international standards.

The International Organization for Standardization (ISO) is the most recognised international institution for industry standards. Regarding cybersecurity, the 2700X family of standards covers all TOM relating to the 'state-of-the-art' of information security [SHB17] (page 63). The German BSI extends the ISO27001 standard through its IT-Grundschutz Compendium covering security recommendations for organisations [SHB17] (page 66). In addition, the BSI releases many technical guidelines on algorithms, risks, protocols, and various other subjects that are widely acknowledged on an international scale [Tah22] (page 7). Across the Atlantic, in the United States of America, the NIST specifications, such as the CSF and the SOC 2, dominate the industry standards landscape for cybersecurity. The CSF is a self-study guide for organisations to start their cybersecurity effort and claim compliance based on a self-certification [NIS23]. SOC conversely is a reporting standard built by the American Institute of Certified Public Accountants (AICPA) to assess the compliance with defined TSC about service commitments of organisations to its customers. The SOC2 report is not meant to guide efforts to build cybersecurity but to write up the existing state of a Service Organisation's TOM to effectively communicate with stakeholders regarding the current state of cybersecurity in an organisation [SOC23]. Organisations with entities in the United States of America often conform to those standards. To exemplify, industry leaders such as Microsoft Corporation and Amazon.com Inc. comply with the ISO27001 and the SOC 2 standards.

1.1.4 Project and Change Management

From a management perspective, Change Management refers to models and strategies that aid employees in accepting new organisational developments [PK23] (page 189). While the often repeated claim '70% of all change management efforts fail' is not directly supported by academic evidence, many practitioners and academics recognise the inherent difficulties associated with change management projects, according to Hughes [Hug11] (page 460). Further, Hughes states that the quantitative measurement of the outcomes of change management efforts and the effectiveness comparison of change management frameworks is inherently unfeasible [Hug11](page 461). However, change management is still the subject of intense academic research and one of the biggest challenges of organisational leaders [PK23] (page 189). Phillips and Klein [PK23] (page 190) analyse scientific literature and conduct a survey amongst practitioners to create a subset of strategies that aid in organisational change efforts and are used in both the literature

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

and practice. Those change management strategies cover "communication, stakeholder involvement, encouragement, organisational culture, vision, and mission" [PK23] (page 194).

1.2 Research Questions

This master thesis will work on the following Research Question (RQ)s:

- **RQ1:** What supporting material guides financial institutions' efforts to become cyber-resilient?
- **RQ2:** Which cyber security measures must financial institutions implement to be legally compliant in Austria in the next three years?
- **RQ3:** Which generic artefact is well suited to guide financial institutions' cyber-resilience efforts?

The first two questions are seen in the context of a literature analysis. The first question is answered by describing supporting material utilised in financial institutions to guide them in becoming cyber-resilient and through a meta-synthesis of reoccurring themes and patterns discovered across supporting materials. The second question is answered through an enumeration of relevant legal norms. The first two questions entail the knowledge base surrounding this thesis.

The third question incorporates this thesis's design science research part as the strongest as it questions the designed artefact. Well-suited in this context refers to three criteria. The first criterion is reducing legal noncompliance risks. The reduction of legal noncompliance risks will be evaluated using the percentage of relevant paragraphs that the artefact covers and the opinion of domain experts. The second criterion is the reduction in cyber-threat risks. The decrease in cyber-threat risks will be demonstrated by mapping the suggested measures within the artefact to the most common threats. The third criterion is the value of the artefact to practitioners as rated by domain experts regarding the contents and format of the generic artefact. To be rated as valuable, the contents must contain all necessary project-related information in a format that is easy to understand and use.

1.3 Objectives of this master thesis

This thesis addresses the compliance with DORA and the step-wise establishment of a successful ISMS within financial institutions. By adhering to the specific requirements of DORA and implementing a robust ISMS, financial organisations, such as banks and insurance companies, can establish a profound cyber-resilience and secure the trust of customers and stakeholders alike.

The expected results of this thesis include:

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

- an understanding of organisational cyber-resilience and its areas of influence
- an overview of research and industry standards surrounding organisational cybersecurity
- an evaluated, granular project plan template that aids organisations in their structured development of cyber-resilience and compliance with cybersecurity regulations.

1.4 Relevance to the Business Informatics MSC Program at TU Wien

In this master's thesis, compliance with EU law regarding cyber-resilience and the setup of cyber-resilience in organisations is further analysed. The following lectures on Business Informatics at TU Vienna are therefore relevant to this thesis:

- **280.118 Advanced Aspects of IT-Law**
  This course covers project law, IT security law, European law and international IT law. The EU and international IT law sections are especially relevant to this thesis.
- **183.633 IT Security in Large IT Infrastructures**
  This course covers security aspects in software projects in large IT infrastructures. Particularly relevant to this thesis are aspects of the security goals and their implementation in large IT infrastructures.

1.5 Significance of this master thesis

The insights gained in this master thesis can build the foundation of ICT projects in organisations in general and financial institutions in particular. This thesis outlines important legal norms and industry standards. It provides a project plan template to comply with legal norms and build organisational cyber-resilience from a practise-oriented perspective. The project plan template is designed to be used with minimal customisation for relevant projects. It has practical significance as it will be used for the author's capacity as an ICT consultant for ICT projects of financial institutions.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

CHAPTER 2

Applied Research Methods

This chapter provides a summary of the academic methods used to conduct this master thesis and how each of them will be applied. The methodological framework for this thesis is Design Science Research.

2.1 Design Science Research

Design Science Research is a methodology introduced by Hevner et al. [HMPR04] page (80). It is used for scientific work in information systems and computer science. The core principle of Design Science Research is creating new knowledge and insights through developing artefacts and their rigorous evaluation [HC10] (page 7). The Design Science Research framework aims to generate usable results that have proven practical applicability and value to real-world problems by gradually improving or introducing new solutions to existing problems. Design Science Research focuses on artefacts such as constructed systems, models, methods, processes or technologies [HMPR04] (pages 82-84). March and Vogus [MV] (page 195) discuss the application of Design Science in management disciplines. This master's thesis uses design science in the context of information systems in organisations; however, the artefact created has substantial parts from the management disciplines. March and Vogus [MV] (page 199) widen the potential artefacts for the management disciplines and specifically mention anything that enables managers to organise, direct, control, and monitor companies' resources, justifying a project plan template as a valid artefact.

Several phases must be followed systematically while utilising the Design Science Research Framework.

The first phase is a detailed identification of the problem. To drill down onto a specific issue, the recent knowledge regarding the selected area of research must be analysed. This phase results in an in-depth analysis and definition of the research problem. This

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

phase will be conducted through semi-systematic literature research and a summary of the most recent industry standards and laws.

The second phase is the requirement engineering of the artefact. The artefact's specific functions, properties and characteristics are defined in this phase. During this phase, the design principles and goals of the artefact design must be determined. The abovementioned requirements are collected and analysed in this phase by aggregating industry standards and legal requirements. The design methods and the concrete form of the artefact (the project plan template) will be developed during this phase.

After carefully selecting and defining the requirements of the artefact and its design process, the artefact is developed in the third phase. The artefact is created during this phase to fulfil the requirements, design principles, and goals. Many tools and methods can be utilised to develop the artefact. This master thesis illustrates an organisation's different steps to create and realign existing cyber-resilience measures in a format that fulfils the defined requirements. The developed project plan template format is potentially an Excel time plan, a project handbook or something similar.

The fourth phase of the Design Science research framework consists of the evaluation and demonstration phase. The artefact must be rigorously evaluated through scientific evaluation methods. Within information systems, those methods are categorised by Hevner et al. [HMPR04] (page 86) as Observational, Analytical, Experimental, Testing or Descriptive. In this master thesis, the evaluation phase consists of an analytical requirements verification and carefully prepared expert interviews with senior management, including CISOs, CTOs and CEOs of banks, other financial organisations or with experience in compliance projects or ICT-related projects. These interviews are made possible by the connections and network in the author's capacity as a consultant.

The last and fifth phase of the Design Science research framework consists of communicating the research project. During this phase, the research project results are documented and published to be shared with other researchers and the scientific community. This last phase of the master thesis consists of the submission of the thesis at the Faculty Of Informatics at the Technical University of Vienna and the Institute of Spatial Planning, where the coordinating professor for IT law, Professor Haslinger, holds the research unit for law. Furthermore, the artefact of this master thesis will be used commercially at the cybersecurity Consultancy 'Certitude Consulting GmbH' in DORA related projects.

Furthermore, Hevner et al. [HMPR04] (page 88) describe Design Science Research as an iterative process. This iterative approach creates the need to revisit the different project phases throughout the research project, necessitating the re-visitation of specific phases. Figure 2.1 shows the Design Science research framework overview. In this master's thesis, the environment consists of the people in a financial institute and their different departments and roles. The change management requirements are essential to the artefact design in the organisation's context. Furthermore, compliance with laws is part of the business needs. Technology is the different information and communication technology assets that any organisation employs.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

The knowledge basis of this master thesis consists of different industry standards that guide artefact development. The existing and newly introduced laws, such as DORA, also contain knowledge about cyber-resilience. Another central factor for the knowledge base is academic research in organisational cyber-resilience. The Development/Build part of this thesis is the project plan template. The Justify/Evaluate part of this thesis consists of qualitative expert interviews and an analytical verification, which are described in the method details section 2.3. The application in the appropriate environment will happen outside the scope of this master thesis. However, the expert interviews are a first step towards its implementation in the proper environment. Additions to the knowledge base from this master's thesis will happen through the publication at TU Vienna.

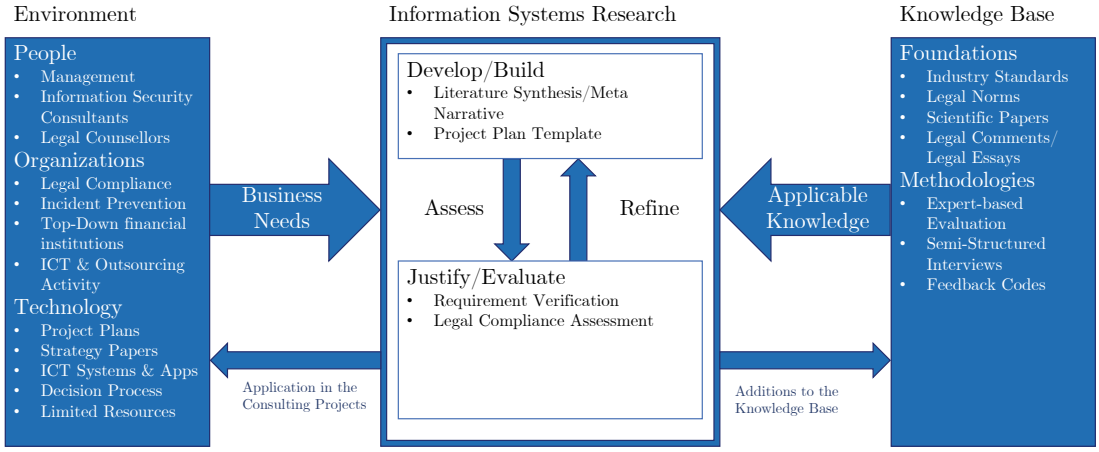


Figure 2.1: The iterative Design Science process instantiated from Hevner et al. [HMPR04] (page 80)

2.2 Literature Review

A literature review is essential to any scientific project, providing an understanding of the current state of knowledge in a specific field. Snyder [Sny19] (page 334) differentiates three different kinds of literature reviews: systematic literature reviews, semi-systematic literature reviews and integrative literature reviews. These three different approaches differ in their target and their field of application. The semi-systematic literature review is used in fields conceptualised differently by diverse disciplines, making a systematic literature review unfeasible [Sny19] (page 336). The semi-systematic literature review aims to understand the different aspects of a topic and creates a meta-narrative that combines the views of other disciplines. In this thesis, the semi-systematic literature review is selected because the field of organisational cyber-resilience is multidisciplinary. The existing research papers each approach the topic from a unique perspective, and the semi-structured literature review allows for the inclusion of a diverse body of knowledge, such as industry standards and laws, all of which are essential parts of the existing knowledge in this area.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

The following steps must be undertaken to conduct a literature review:

- **Designing the Review**
  The purpose, scope, and specific research questions for the semi-systematic literature review are created at this stage. In this thesis, the scope will contain organisational measures for cybersecurity and change management.
- **Conducting the review**
  In this stage, the actual review is conducted. The search terms are inserted into different databases, and the resulting articles can be relatively freely selected (as compared to the systematic literature review). In this phase, the documentation of input chosen is essential. As appropriate, a complete reading of these articles or a shortened method can be used to understand the research papers.
- **Analysis**
  The selected papers are analysed during the analysis phase to answer the research questions. In the semi-structured literature review, the analysis methods can be more creative than the statistical aggregation of results. Snyder explicitly mentions the inclusion of material cited in the selected papers [Sny19] (page 337). Any gaps in the research and gained meta-knowledge or models should be documented. In this master thesis, a model of the different areas of organisational cybersecurity, such as Business Continuity, Asset Management, Physical security, etc., likely results from the analysis phase.
- **Writing the Review**
  In the last phase of the literature review, the insights gained are documented by explaining the findings and the identification, analysis, synthesis, and reporting process. Specifically, conceptual models and categorisations are mentioned as possible results. The visualisation of the model of areas of organisational cybersecurity could be part of the writing phase.

2.3 Qualitative Evaluation: Semi-Structured expert interviews

The methodology of expert interviews is applied from the description of Turner [Tur10] (pages 754-759) and Bogner et al.[BLM09] (pages. 27-83).

Turner [Tur10] (pages 755-756) describes expert interviews in three different categories:

- **Informal Conversational Interview**
  This approach relies upon spontaneous interaction with participants. This approach leaves the content of conversations widely open and depends on the proper context setting and participant selection to conduct research. For this master thesis, an unstructured approach will not be used because specific answers to the qualities of the artefact are relevant to the research questions.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

- **General Interview Guide Approach**
  This semi-structured approach leaves the interviewer in the driver's seat using prepared topics and loose questions, allows asking questions in different styles, allows for follow-up questions and the adaptation of the interview structure. This approach considers the setting of each interview and can help build a comfortable setting with participants. In this master thesis, the goal of the interview is to evaluate the artefact. However, this method may lead to diverse results and could introduce bias towards critics that the author prefers among the participants.

- **Standardized Open-Ended Interview**
  In this well-structured approach, the interviewer has a set of questions that are posed as similarly as possible from participant to participant, and they are open-ended. The open-ended questions allow participants to go into as much depth as they want. The standardised questions minimise researcher bias and offer a clear interview evaluation. This approach will be used during the master thesis. In preparation for the interview, the experts receive the developed artefact and are then interviewed about the different quality criteria and requirements associated with the artefact.

According to Turner [Tur10] (pages 757-759), the three different steps to conduct qualitative interviews consist of:

- **Preparation**
  The preparation includes selecting participants, planning the interview phases and piloting the interviews. The participant selection should be made with a method such as criterion selection or critical case sampling. According to Turner [Tur10] (page 757), critical case sampling is used in cases where only a small number of participants can be expected. In this master thesis, the number of willing top-level managers (CEO, CTO, CISO) is expected to be limited; therefore, this approach will be used. The interview should be held at a place with little distraction. During the interview process described by Turner [Tur10] (page 757), the researcher should explain the purpose, address terms of confidentiality, explain the format of the interview, indicate the length of the interview, offer a post-interview contact possibility and ask for questions before the interview starts. The researcher must not rely on his memory to recall the answers to questions but record them. In this master thesis, the interviews will be held in virtual meetings and the participants' offices. As the purpose is to evaluate the artefact, the interviewees will be offered relative anonymity and the possibility to edit their answers. They will also have the chance to contact the interviewer by phone and e-mail, and the interviews will be recorded with a voice recorder, but the recordings will not be submitted to ease the participants' rapport.

- **Constructing Effective Research Questions**
  To construct the research questions, Turner [Tur10] (pages 757-758) mentions the

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

following guidelines. Effective research questions include:

- using open-ended questions
- using neutral wording
- not mixing questions
- clear wording including applicable terms
- avoiding 'Why?' questions when possible

Furthermore, Turner [Tur10] (page 758) suggests preparing follow-up questions to redirect participants' focus onto the intended topic.

- **Actual Implementation**
  During the interview, Turner [Tur10] (page 759) stresses the importance of checking recording devices, asking one question at a time, remaining neutral, encouraging responses through mimicking, avoiding obvious note-taking, providing transitions between topics and staying in control.

2.4 Design Verification

The fulfilment of requirements as laid out in chapter 5 is verified through analytical methods. Analytical evaluation is suggested by Hevner et al. [HC10] (page 119) as one possible evaluation method. Different Key Performance Indicator (KPI) coverage percentages are calculated and compared to determine the fulfilment of legal obligations, state-of-the-art ICT landscape, internal governance, and cyber threat reduction. To compare the state-of-the-art ICT landscape, the project plan template is mapped to an industry standard, and similarity scores are calculated.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

CHAPTER 3

Semi-Systematic Literature Review

3.1 Purpose and Scope

All research questions from the master thesis are, to some extent, addressed in the literature review. The first question outlines the legal aspects of financial institution's cyber-resilience. The second question focuses on organisations' current guidelines and organisational security frameworks. Besides legal norms, the second research question deals with existing guidelines, frameworks and industry standards. As some legal norms refer to the state of the industry or state of the art, those standards have legal importance.

3.2 Conducting the Review

3.2.1 RQ1: Legal Compliance

The Austrian and EU jurisdictions are analysed for applicable laws, directives, and regulations regarding financial institutions' cybersecurity. For the EU jurisdiction, the starting point will be the official EUR-LEX database, run by the Publication Office of the European Union. For the national-Austrian - level, the Rechtsinformationssystem des Bundes (RIS) will be used as a starting point.

All legal norms that address information security and IT assets are included. Legal norms that do not apply to financial institutions in Austria, that do not provide details on security requirements or are only relevant for a small fraction of financial institutions' business, such as algorithmic trading or blockchain technologies, are excluded.

As found in Regulation (EU) No 1093/2010 on the competencies of Supervisory Authorities, the EBA releases a set of technical guidelines relevant to all banks operating in the

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

European Union (EU). Hence, the relevant guidelines of the EBA are included in the literature review.

3.2.2 RQ2: Cyber-Resilience Guides

For the second research question, academic papers that contain empirical data regarding the usage of frameworks and standards are analysed. The empirical studies in scope are meta-analysis or market research. Included Databases for this literature review are ResearchGate and ACM Digital Library.

This literature review includes papers written in the last 8 years, cited more than 10 times and comparing information- or cybersecurity frameworks, standards or guidelines. References from the papers already included are also considered potentially relevant and included in the compilation. The relevance is determined ad hoc, and the analysis of search results is not exhaustive, following the chosen semi-systematic literature review approach as described in section 2.2. Papers that are not published in relevant journals are excluded. After the initial inclusion, another selection is carried out based on the abstracts of the selected paper. Finally, all pertinent frameworks and other relevant findings to RQ2 are summarised.

3.2.3 RQ3: Abstract Guiding Artifact

For the third research question, the 'International Journal of Project Management' is a starting point for the literature research. Since Project Management is a more mature scientific discipline than cybersecurity, papers published within the last 20 years are included. Papers must contain insights about failure or success factors within project management and must contain insights about a guiding artefact such as a project plan. Work cited in the included papers may also be incorporated. The insights from the literature research on guiding artefacts are gathered to develop requirements in the next chapter.

3.3 Analysis

3.3.1 RQ1: Legal Compliance

The following legal norms are relevant to financial institutions' cybersecurity and will be further analysed.

1. **NIS2** replacing NIS1 and the derived national implementation Netz- und Informationssystemsicherheitsgesetz (NISG).
2. **DORA** and associated regulatory technical standards.
3. **Revised Payment Services Directive (PSD2)**, in particular chapter 5 and the derived national implementation Zahlungsdienstegesetz (ZaDiG).

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

4. **EBA Guidelines on ICT and security risk management (EBA/GL/2019/04)**.
5. **EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)**.

The concrete cybersecurity measures to be complied with are not cited but analysed and marked as such throughout the entire thesis. A summary of the respective norms is given in the following paragraphs.

Revised Payment Services Directive (PSD2) In chapter five of PSD2, several aspects of cyber-resilience are mandated for payment service providers. This includes the establishment of an ICT security framework, an incident management system, ICT-Risk and ICT-Incident reporting, and end-user authentication requirements.

European Banking Authority (EBA) Guidelines on ICT and security risk management (EBA/GL/2019/04) This publication of the European Banking Authority is mandated through Article 95 of the PSD2 and addresses payment service providers, credit institutions and investment firms. It touches on the following topics relevant to cyber-resilience:

- Internal governance regarding information security such as budgeting, strategies, policies, processes, roles, responsibilities, governing principles
- Staff requirements, awareness and training
- Third-party providers: Service Level Agreement (SLA), TOM, incident handling and reporting
- ICT Risk management process
- Asset Management and Dependencies between assets, roles and processes
- Business Impact Analysis and Classification
- Internal Reporting and Auditing
- Physical Security and Cryptography
- Vulnerability-, Incident, Patch-, Configuration-, Change-, Project-, Lifecycle- and Capacity-Management
- Technical and Logical Security Measures such as firewalls, segmentation and Data Loss Prevention (DLP)
- Security Monitoring, Incident Management
- Response and Recovery Processes, including Backup planning and communication plans

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

- Security Testing and Plan Testing
- ICT systems acquisition and development
- Business Impact Analysis (BIA) and Business Continuity Management (BCM)
- End-user training and End-user security awareness

European Banking Authority (EBA) Guidelines on outsourcing arrangements (EBA/GL/2019/02) The EBA guidelines on outsourcing arrangements direct how credit institutions, investment firms, payment institutions and electronic money institutions may use third parties to support their business processes, including outsourcing to cloud service providers. Within the guideline, financial institutions in scope must fulfil the following topics regarding outsourcing:

- Internal strategies, policies, roles and responsibilities regarding outsourcing
- Risk Assessments and Due Diligence
- Classification of outsourcing as critical and important, the associated dependencies and the associated risk
- Internal processes, including selection, approval, monitoring, auditing and documentation of third parties
- Business Continuity Management, Oversight and Exit Strategies
- Contractual Requirements including TOM regarding Information Security, Audit Rights, Reporting, Testing and Termination Rights

Directive on measures for a high common level of cybersecurity across the Union (NIS2) The European institutions adopted NIS2 into effect in January 2023. EU Member states have until mid-October 2024 to implement the Directive and put it into effect on the national level. The Directive aims to strengthen the cybersecurity of critical services in key sectors such as energy and banking. The following categories of TOM for affected organisations are listed in the NIS2:

- Top Management commitment and accountability
- Internal policies regarding information security
- Incident Handling
- Business Continuity
- Third Party Risk Management

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

- Supply chain security
- Operations Security
- Vulnerability Management
- TOM effectiveness evaluations
- End-user security guides and training
- Cryptography
- Human resources security
- Access control policies
- Asset management
- Multi-factor authentication or comparable mechanism
- Secured (emergency) communications
- Physical security

Digital Operational Resilience Act (DORA) DORA is the most current piece of legislation regarding the cyber-resilience of financial institutions and aims to make the EU's financial system more resilient to cyber threats and ICT disruptions by regulating how financial institutions use and live with ICT. As such, DORA is the broadest regulation in this thesis, both in scope and content. According to recital 3 of the DORA, approximately 22,000 entities fall under the scope of financial institutions in the EU. The norm went into effect in January 2023 and will become enforceable as of January 2025. According to recital 16, DORA is a *lex specialis* to NIS2, thereby supplanting NIS2 for financial institutions. It is further extended with three Regulatory Technical Standards (RTS) and one Implementing Technical Standards (ITS) to be published by the European Supervisory Authorities (ESA) Joint Committee [Ös23] until January 2024 and further Technical Standards until July 2024. As of October 2023, the following draft versions of the Technical Standards have been released and are included as such:

- Consultation paper on draft RTS ICT risk management tools methods processes and policies
- Consultation paper on draft RTS on classification of ICT incidents
- Consultation paper on draft ITS on register of information
- Consultation paper on draft RTS on policy on the use of ICT services regarding critical and important functions

A more detailed view of the background of DORA is found in section 4.4.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

European Network and Information Security Agency (ENISA)

3.3.2 RQ2: Cyber-Resilience Guides

The following frameworks are mentioned in academic papers as being used by practitioners or viewed as central to organisational cybersecurity. They are summarised in the following paragraphs. The content of those frameworks regarding TOM, processes, policies, et cetera are used throughout the whole thesis and marked accordingly.

International Organization for Standardization (ISO)27001 The ISO27001 standard is central to the development of organisational information security [VE07] (page 3), [PLS20] (page 1), [Nic18] (page 15), [HHC23] (page 689), [DW14] (page 3), [MS22] (pages 1-2). The ISO27001 standard is an international industry norm regarding information security management. It defines how organisations build and operate an Information Security Management System to protect data confidentiality, integrity, and availability by following a risk-based approach. Organisations can acquire a certification to display conformance to the industry standard [ISO22]. The three typical security goals - confidentiality, integrity, and availability - are also called the CIA-triad of information security. The most current version ISO27001:2022. It includes minor updates, i.e. Secure Coding and Cloud Computing, compared to the 2013 version.

Control Objectives for Information and Related Technologies (COBIT) COBIT is a framework for IT governance and management. It is not specific to information security but incorporates many aspects commonly consolidated within the information security domain, such as business continuity, risk management and security. The three dimensions that COBIT describes in detail are IT Processes, Business Requirements and IT Resources [MS22] (page 2). It supports organisations in the governance and management of IT systems and processes. COBIT divides IT into domains, emphasises processes and controls and aims to bring organisational targets and IT in line [HDHJVG18] (page 5335). Its current version is COBIT 2019 [cob23]. The five domains are:

- **EDM:** Evaluate, Direct and Monitor
- **APO:** Align, Plan and Organize
- **BAI:** Build, Acquire and Implement
- **DSS:** Deliver, Service and Support
- **MEA:** Monitor, Evaluate and Assess

The exact contents of the 2019 COBIT core model are shown in figure 3.1.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

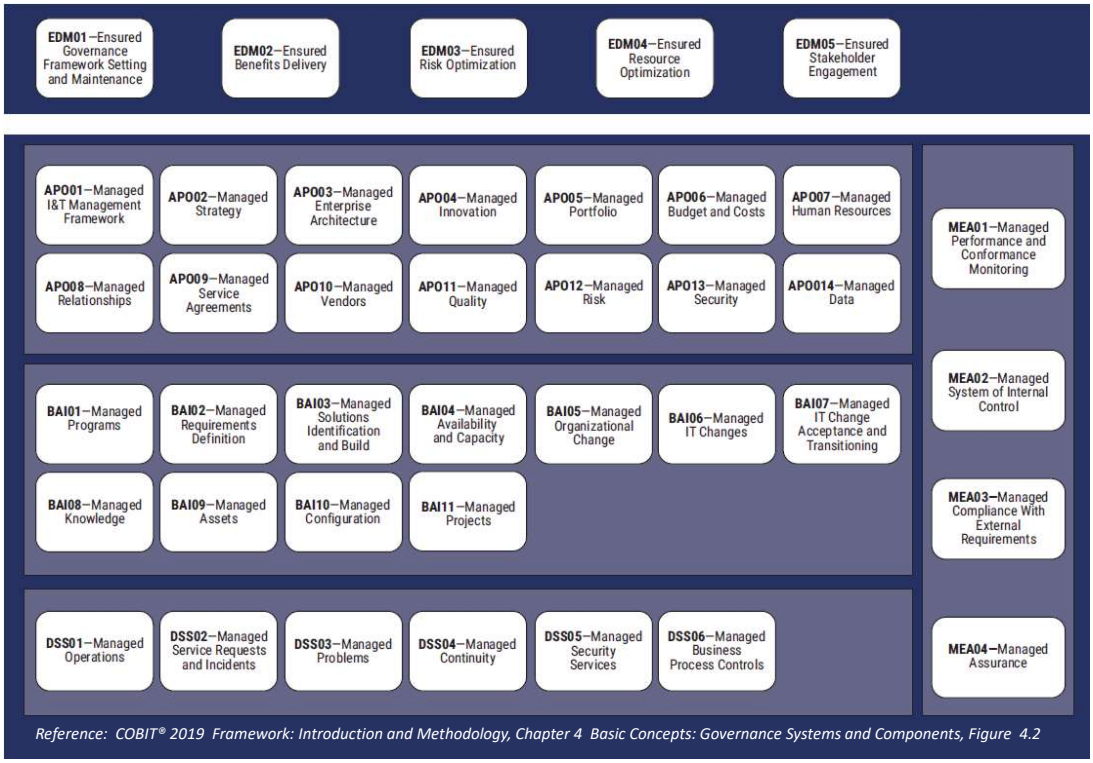


Figure 3.1: The COBIT Core Model from ISACA [cob23]

Information Technology Infrastructure Library (ITIL) ITIL is a collection of best practice management processes regarding IT-Service Management. ITIL Version 4 is the defacto standard of service management [Nic18] (page 5), [HHC23] (page 682). ITIL4 describes 34 practices ranging from standard management to service and technical management practices. Each practice is described across the six activities, from planning, design and transition to operations, improvement, and support. Furthermore, ITIL 4 defines guiding general principles to aid organisations in their process management [Axe19]. While ITIL is not security-oriented per se, it entails many processes relevant to information security, such as Information Security Management, Risk Management, Service Continuity Management, and Incident Management [Nic18] (page 16). Within the ITIL4 framework, three categories of management practices are described: General, Service, and Technical management practices.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) The COSO framework describes how organisations can implement and maintain an efficient internal control system that can also be used to support and implement the internal controls regarding information security[HHC23] (page 716). Within COSO, the internal control system comprises the following components: control environment, risk assessment, control activities, information & communication and monitoring activities. The System

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

and Organization Controls 2 audit standard is one extension of the COSO framework regarding cybersecurity. Within SOC 2, the principles of COSO are interpreted in the context of information security using the Trust Service Criteria [SOC23].

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) The CSF is a voluntary guidance published by the US-American NIST, which is based on existing guidelines and best practices, to manage and reduce the exposure to cybersecurity risk and to standardise communication about cybersecurity risk[HHC23] (page 682). It describes five areas where cybersecurity activities fall: Identify, Protect, Detect, Respond and Recover. Within the five areas, 23 categories and 108 subcategories are identified. The subcategories are mapped onto similar TOM and processes from other frameworks and standards (mostly COBIT 5 and ISO27001:2013). In comparison to the ISO27001 and to COBIT, the CSF offers a very flexible approach and provides a practical method to measure and prioritise risk[NIS23]. At the time of writing, version 2.0 of the CSF was still a draft. Hence, version 1.1 is discussed in this work.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30/39/53 The NIST-800 group publishes documents as standards directed towards federal agencies of the US related to different cybersecurity topics. Their publications “Guide for Conducting Risk Assessments”, “Managing Information Security Risk’ and “Security and Privacy Controls for Information Systems and Organizations” all relate to information security risk management. These publications are voluntarily used or contractually obligated to comply with civil organisations in the US and abroad [MS22] (page 2). The "Guide for Conducting Risk Assessments" (SP 800-30) describes three "Tiers": the organisational level, the business level, and the information system level [SP821] (page 17) on which risks are assessed. The "Managing Information Security Risk" (SP 800-39) follows this three-tier approach and defines different roles and responsibilities for relevant information security personnel and management personnel [Ini11] (page B1-B13). The "Security and Privacy Controls for Information Systems and Organizations" (SP 800-53) is a catalogue of TOM based on the three-tier system and defines 20 areas of TOM with countless subcategories of TOM to secure Information Systems and Organizations against different kinds of threats [For20] (page 16-373). The three-tier differentiation can be seen in figure 3.2.

Payment Card Industry Data Security Standard (PCI DSS) The PCI DSS defines 12 requirements for organisations to comply with. They are designed for the payment card industry but have applicability beyond the card-issuing institutes, setting standards in the field of information security with significant overlap to the controls mentioned in ISO27001 [Nic18] (page 5). The 12 requirements, well-documented and containing detailed sub-requirements [Cou23] (pages 36-333) are as follows:

1. Install and Maintain Network Security Controls.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

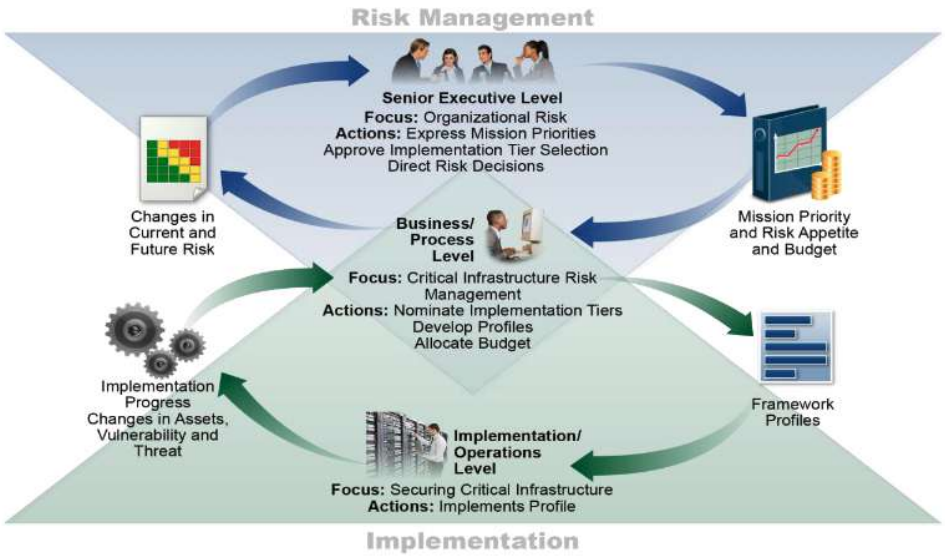


Figure 3.2: The three Tier separation according to the NIST CSF [oST18] (page 12)

2. Apply Secure Configurations to All System Components.

3. Protect Stored Account Data.

4. Protect Cardholder Data with Strong Cryptography during Transmission over Open, Public Networks

5. Protect All Systems and Networks from Malicious Software.

6. Develop and Maintain Secure Systems and Software.

7. Restrict Access to System Components and Cardholder Data by Business Need to Know.

8. Identify Users and Authenticate Access to System Components.

9. Restrict Physical Access to Cardholder Data.

10. Log and Monitor All Access to System Components and Cardholder Data.

11. Test Security of Systems and Networks Regularly.

12. Support Information Security with Organisational Policies and Programs.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Sherwood Applied Business Security Architecture (SABSA) The SABSA is a British model and methodology to build a risk-based information security architecture for enterprises [SCL09] (page 1). It describes itself as an overarching framework enabling integration of "all other existing standards" [SCL09] (page 1) in the domain of information risk and information security. According to Herath et al., [HHC23] (page 690) SABSA is a highly relevant and applicable framework for organisations. The SABSA entails a layered view of information security and differentiates six different architecture layers: contextual, conceptual, logical, physical, component and management architectures. For each layer, the SABSA framework defines the dimensions: assets, motivation, process, people, location and time [hSIAB18] (page 7).

3.3.3 RQ3: Abstract Guiding Artifact

The RQ3 investigates project management and the corresponding documents that lead to success. The success of an IT project can be measured along different dimensions such as the implementation process, the perceived value [DRS03] (page 90), timeliness, costs, employee satisfaction, management satisfaction, client satisfaction, and on an individual basis depending on the sector [HA04] (page 508). One study finds that the time spent implementing project planning and procedures does not correlate with overall project success. However, defining a project's requirements correlates highly with project success [DRS03] (pages 94 and 95). Dvir et al. [DRS03] (page 89) suggest spending plenty of resources on the requirement and goal definition. Tasevska et al. [TDD14] (page 536) demonstrate that formulating a baseline plan is a crucial success factor for overall project success while developing a solid business case aids during the implementation process of an IT project. Ngai et al. conducted a meta-study regarding critical success factors in project management across global regions. Concerning the requirements of a guiding document in Europe, the following factors stand out: creating a clear vision and a justification, interdepartmental communication, benchmarking progress against milestones or performance metrics, project champion, project management and a clearly defined project plan containing project goals [NLW08] (pages 552-554). Sicotte & Delerue point out that overdoing the upfront planning of uncertain projects leads to dissatisfying results of projects [SD21] (page 2). Varajao et al. [VLG22] (page 1) state that a common *project management success* definition consists of complying with time, scope and costs, while *project success* is creating stakeholder satisfaction or business benefits. While project management success can be measured at the end of a project, project success can only be measured at some point after the project is finalised. La Paz & Lopez [LPL23] (page 1939) state the typical IT project management dimensions are budget, people, risk, communications, documentation, and scope. Kaufmann & Kock [KK22] (page 625) demonstrate a causal relationship between project management efforts and commercial project success, especially on large, complex projects.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

3.4 Synthesis and Meta-Narrative

In this section, the insights from the literature review and identified reoccurring patterns are described.

3.4.1 Project Management

The literature on the last research question revealed that most project management research comes from implementing Enterprise Resource Planning systems or software development projects. The literature presents success factors, definitions of project and project management success, and finally describes the project plan as the artefact that guides organisations through projects. Project plans are made upfront of a project. The literature suggests elements that should be integrated into a project plan, such as risk management, definitions of success and milestones.

3.4.2 Integration of Findings from Different Disciplines

After careful analysis of the literature regarding norms and frameworks for information security, the following integration of those two disciplines is developed: the different areas of information security can be distinguished into three separate layers following the Three Tiers from the NIST CSF:

- The **Organisational Layer** contains measures carried out by senior management and specialised organisational units on a governance level. Exemplary measures for this layer include creating an information security strategy and defining roles and responsibilities.
- The **Process Layer** contains processes. Exemplary measures on this layer include Business Continuity Management and Asset Management. The measures in this task are typically carried out by IT-related management personnel or IT specialists.
- The **Implementation Layer** contains all the technical measures to protect ICT. IT specialists or the operation teams carry them out and include the technical implementation of the processes, artefacts and policies defined by the other two layers. Examples of measures on this layer include firewall implementations and physical security measures such as fencing or video surveillance.

3.4.3 Conceptual Model or Framework Developed

The following graphical model 3.3 includes the reoccurring patterns identified during the literature review analysis and a distinction of the activities surrounding cyber-resilience.

3.4.4 Identification of Gaps in Research

Selecting an appropriate information security framework is not easy, and none of the discovered papers provide or reference a method to choose a proper framework from the

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

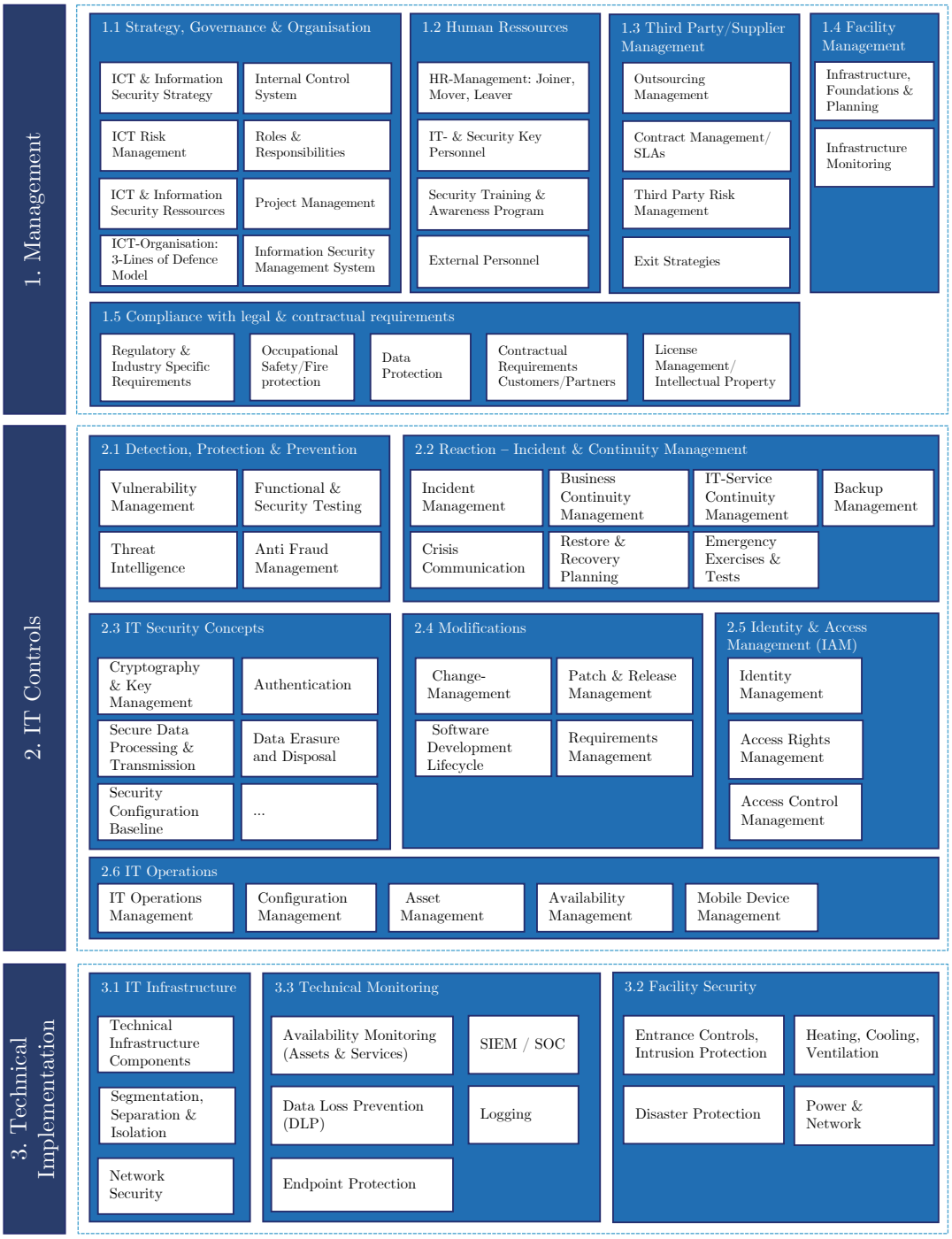


Figure 3.3: Areas of Influence of Information Security. Source: Created by the author.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

large pool of available frameworks. The discovered comparison of frameworks in the literature is also limited to a small subset of all available standards. Furthermore, no census or comparable extensive data is available regarding different information security frameworks, making it difficult to understand how widely different frameworks are used. It is suspected that organisations choose their information security frameworks based on the previous experience and background of the practitioners involved, as well as the organisation's type, size and geographical location. Furthermore, as the legal norm DORA is relatively new, and the relating RTS and ITS are just released as drafts, their final form and their impact remain to be seen.

3.5 Conclusion

3.5.1 Summary of the Review Process

During the review process, legal norms are researched and summarised. Common ICT security frameworks are listed and outlined. Some current findings of project management in the academic literature regarding project success and project planning contents are presented. The found material is synthesised, and a graphical representation that categorises reoccurring patterns is developed.

3.5.2 Key Findings and Contributions

Since there are many different frameworks, selecting one security framework is a non-trivial task for organisations. Most frameworks and norms have highly reoccurring patterns and areas of application when it comes to protecting information, ICT-systems and ICT-supported business functions. Financial institutions have various norms in the area of cyber-resilience to comply with, the most recent and substantial being DORA and its surrounding RTS and ITS. A project plan template is one abstract artefact that guides organisations through their cyber-resilience efforts.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

CHAPTER 4

Understanding Systemic Digital Operational Resilience

This chapter of the master thesis is an essay on the concept of resilience. It deepens the understanding of resilience in different scientific disciplines and on systemic scales. It further explains why the EU developed the DORA to strengthen the financial sector's cyber-resilience.

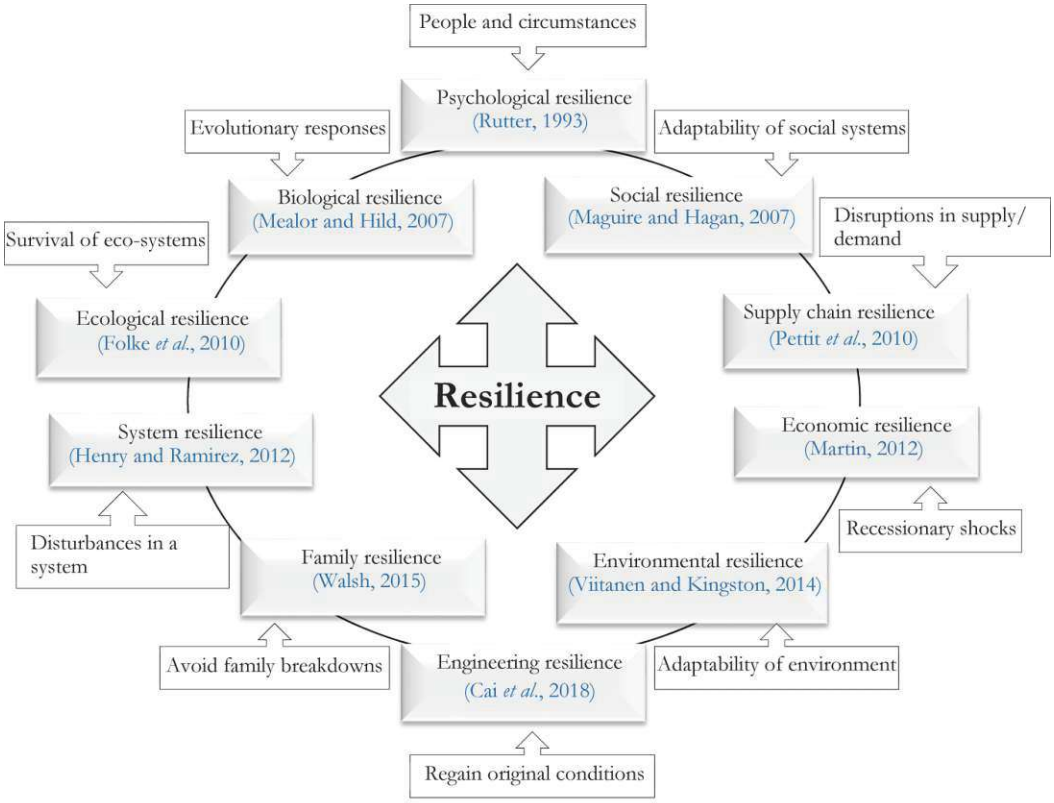
4.1 Resilience in other Disciplines

"It ain't how hard you hit; it's about how hard you can get hit, and keep moving forward. How much you can take, and keep moving forward." - Sylvester Stallone, in Rocky VI. This quote from the pop-cultural American sports drama Rocky VI showcases that resilience is deeply ingrained into society's intuitive evaluation of strength. It is unsurprising to find the concept used across many scientific disciplines. The following subsections provide an overview of the term resilience in scientific disciplines other than ICT. The meta-analysis from Shishodia et al. [SSRM21] (page 883) conceptualised the different areas of resilience, as seen in figure 4.1.

4.1.1 Resilience in Material Science

Resilience originates from material science as a physical property of substances and structures. Within material science, the meaning of resilience has changed over the last two centuries. Ultimately, the definition resulted in the capacity of a material to take up shock without permanent deformation [Thu84] (page 251). This definition already contains two parts: resisting change and returning to a previous state. A material that takes up shock with minimal deformation, such as a rock, has a high resilience until the shock becomes big enough to deform the rock permanently. Very elastic materials such

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN



Note(s): References in the figure are provided in the extended list of references

Figure 4.1: Different areas of resilience in the literature according to Shishodia et al. [SSRM21] (page 883)

as sponges can take up shocks with large temporary deformation but will return to their original state once the pressure or shock is absent.

Resilience in materials is a determining factor and of great economic value. Modern research regarding the resilience of structures happens predominantly within fields such as physics, chemistry, biology and engineering. One such example is the research of Burla et al. [BMV+19] (page 1) on biopolymer networks' mechanical resilience and active material properties. They investigate the mechanic properties, such as the mechanic resilience of biological structures. Specifically, they research the relationship between withstanding shock and the ability to adapt and self-heal in biological structures such as cytoskeletons and extracellular matrices. A cytoskeleton is the structure that keeps the form of one cell. At the same time, an extracellular matrix is the structure that maintains the integrity and structure of tissues consisting of multiple cells. Another example of resilience research in material science is the research of Mebarki [Meb17] (page 426-427), who developed a framework to measure structural resilience. He compared resilience from different disciplines and developed a framework and a set of metrics for measuring

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

structural resilience. His definition of resilience is shown in figure 4.2. It consists of several components:

- An utility function of a system describing its capacity to supply value at any time t as R(t).
- R_{Min} as the point in the utility function below which a system no longer survives, as it no longer provides sufficient utility. Any utility value between R_{Min} and R_{Opt} is considered optimal.
- R_{Opt} as the optimal point of the utility function above which the system is considered supra-resilient or over-engineered.
- An initial stress at point $t_{d,i}$ up to point t_d
- Three resulting utility functions upon which systems are either considered over-resilient(I), non-resilient(II) or resilient (III)

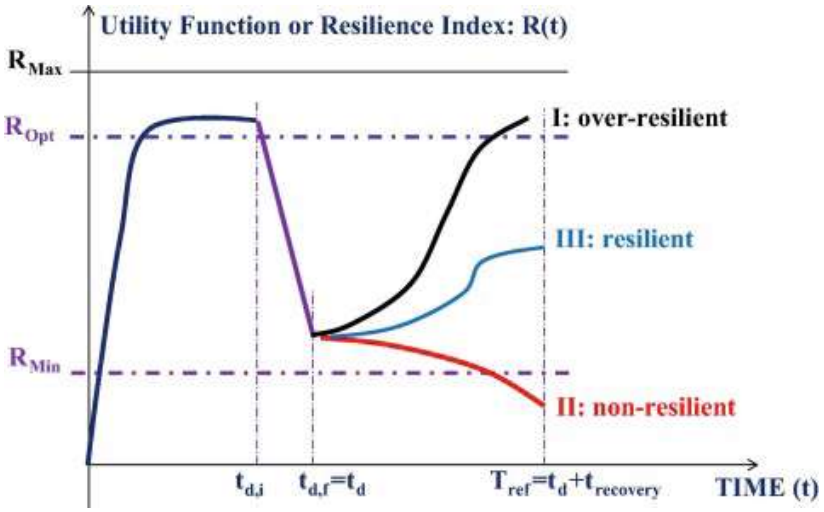


Figure 4.2: Resilience evolution vs. time. From Mebarki [Meb17] (page 426)

The resilience framework of Mebarki [Meb17] (page 426) helps determine the resilience of systems outside the material science from where it results. Determining the utility of any system after the stress has occurred is a critical thought in resilience terms across scientific disciplines.

4.1.2 Resilience in Psychology

This subsection details the concept of resilience as used in the scientific discipline of psychology. Resilience, in general, is described by the American Psychology Association (APA) as the ability to adapt in the face of tragedy, trauma, adversity, hardship, and

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

ongoing significant life stressors[New05] (page 227). Further, psychological resilience influences health, well-being, an individual's quality of life and how they react to the challenges of ageing [WBN11] (page 1). Resilience is often associated in psychology with the ability to cope with stress [CD03] (page 76). Connor and Davidson [CD03] (page 76) argue that resilience entails personal qualities that allow one to thrive in the face of adversity. The best-rated measurement scale to determine and compare resilience in individuals is the Connor-Davidson Resilience Scale (CD-RISC)[WBN11] (page 14). The CD-RISC, as described by Connor and Davidson [CD03] (page 78), lists 25 items as indicators for resilience of individuals:

1. Able to adapt to change
2. Close and secure relationships
3. Sometimes fate or God can help
4. Can deal with whatever comes
5. Past success gives confidence for new challenges
6. See the humorous side of things
7. Coping with stress strengthens
8. Tend to bounce back after illness or hardship
9. Things happen for a reason
10. Best effort no matter what
11. You can achieve your goals
12. When things look hopeless, I don't give up
13. Know where to turn for help
14. Under pressure, focus and think clearly
15. Prefer to take the lead in problem-solving
16. Not easily discouraged by failure
17. Think of oneself as a strong person
18. Make unpopular or difficult decisions
19. Can handle unpleasant feelings
20. Have to act on a hunch

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

21. Strong sense of purpose
22. In control of your life
23. I like challenges
24. You work to attain your goals
25. Pride in your achievements

All those items described in CD-RISC are resources that enable individuals to cope, adapt and overcome disruptions and stress events [WXY+23] (pages 1-2). According to Wang [WXY+23] (page 2) et al., the CD-RISC is linked with the quality of life, depression, frailty, physical activity, sedentary behaviour, strength, optimism and tenacity.

4.1.3 Resilience in Legal Norms

To understand the use of the term Resilience in the legal community, the following databases are queried for the term' resilience' and filtered for legal content: "beck-online", "JSTOR", "degruyter" and "wiso-net". The results can be roughly categorised in the following areas: ICT, education[PdK23], public health [EU-23] (page 1), [MdIdLNW23], biosystems [GGBB20] (page 319), economies[Rat23b][Res23a] and psychology [HDF14] (page 215), [Kuh13] (page 110).

One appearance regarding ICT is made in the GDPR in Article 32 Section 1(b) referencing it on the same level as confidentiality, integrity and availability - the classic IT Security goals [GHR18] (page 1).

A definition of resilience is stated in Article 2 (2) of Directive (EU) 2022/2557 'on the resilience of critical entities' as:

'resilience' means a critical entity's ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident

According to the US inter-agency paper titled "Sound Practices to Strengthen Operational Resilience"[Str24] (page 2) operational resilience "is the ability to deliver operations, including critical operations and core business lines, through disruption from any hazard. It results from effective operational risk management and sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions."

4.2 Systemic Resilience

This section describes resilience in larger systems beyond physical material or single entities.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

4.2.1 Resilience in Ecosystems

Holling [Hol96] (pages 31-38) lists differences in ecosystems from engineered systems. Amongst others, ecosystems change episodically and not gradually; linearity is not a given; several ecosystem equilibriums exist, and fixed rules and management practices towards ecosystems reduce ecological resilience. Further, Holling describes differences from an engineering perspective on resilience, which he calls "fail-safe" and a biologist's evolutionary perspective, which he calls "safe-fail" [Hol96] (page 33). The engineering perspective is closely related to the aforementioned Resilience concepts of 4.1.1 and 4.1.2.

Resilience in ecosystems is, according to Adger [Adg00] (page 349-350), related to the functioning of the system as a whole, while the stability of parts and the stability and maintenance of a stable ecological state play no role in the concept of resilience when applied to ecosystems. Adger reviews different definitions of ecological resilience on the level of ecosystems and summarises the literature in two ways. One view of ecological resilience is the resistance needed until an ecosystem permanently changes its dynamic equilibrium. This permanent change is defined as changes in variables and processes that determine behaviour for the component populations. Another definition of resilience in ecosystems is related to the speed of recovery from stress, in contrast to resistance, which is the actual impact realised from stress. Figure 4.3 displays both definitions of resilience. The second definition closely resembles engineering resilience as stated by Holling [Hol96] (pages 31-38) and Wieland and Durach [WD21] (page 316-320).

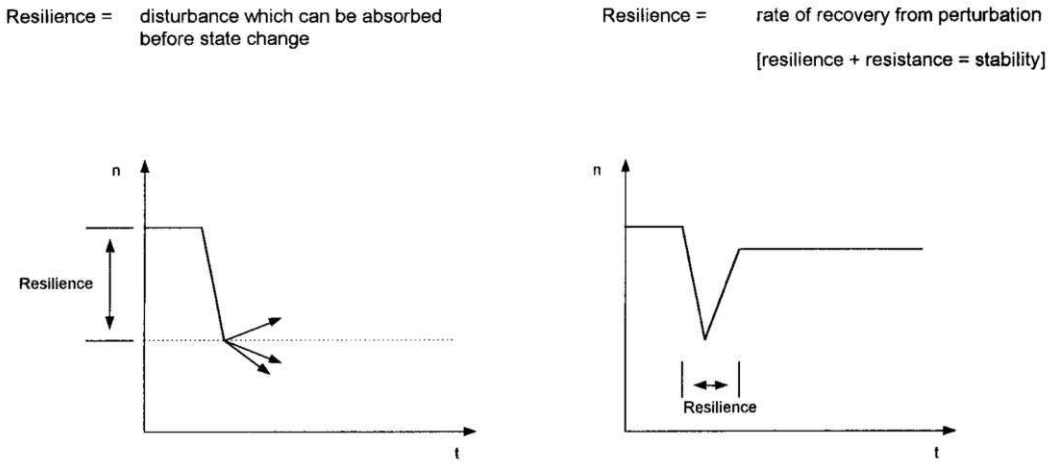


Figure 4.3: Ecological resilience. Contrasting view as presented by Adger [Adg00] (page 350)

Ecologists argue that resilience is the key to conserving terrestrial biodiversity from artificial change processes such as climate change [Adg00] (page 361). Adger further states that the resilience of ecosystems is one crucial component of sustainability in the broader sense. Stability and resistance are not necessarily desirable from an evolutionary point of view.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Gunderson et al. [GAH09] (pages 429-433) describe ecosystems changing in four phases. The first phase is the growth phase; in ecosystems, it is usually primary or secondary succession in territories. This phase is marked by an accumulation of capital and structure in the form of biomass. The second phase is the maturation phase, during which ecosystems grow less rapidly, and more connections and high diversity in components appear. The third phase is the conservation phase, during which resources are mainly used to maintain the system instead of growing, and the system becomes increasingly interconnected. During the conservation phase, the system becomes vulnerable to external disturbances. The last phase appears during stressful periods of rapid destruction, such as wildfires and pest outbreaks. The last phase is marked by creative destruction - the evolutionary cycle begins anew. In this context, ecological resilience defines an ecological system's ability to remain within or return to a functional state of said ecosystem with a similar set of variables and processes throughout this change cycle. Gunderson et al. [GAH09] (page 435) discuss the undesirability or desirability of resilience from an evolutionary point of view. A desired system is challenging to define in detail, and such a definition, once found, can change over time.

4.2.2 Resilience in Supply Chains

Wieland and Durach discuss resilience in supply chains and highlight meanings in other disciplines [WD21] (pages 315-320). They contrast engineering and ecological resilience, with the first having a strict equilibrium state that a system should 'jump back' to and the latter having a more general persistence and adaption of an organism or a system to survive and thrive. Applied to supply chains, they conclude that engineering resilience has been used in the literature in the past. Yet, ecological resilience is more fitting to apply to complex global supply chains. However, they add a social actor component into the resilience view to what they call social-ecological resilience. The social addition entails the possibility of social actors planning and adapting, thereby actively facilitating the transformation of systems in opposition to reactive actors, such as plants, which lack the proactive capacity to plan and adapt. Wieland and Durch (2021) define supply chain resilience as "Supply chain resilience is the capacity of a supply chain to persist, adapt, or transform in the face of change." [WD21] (page 316). In their meta-analysis, Shihodia et al. [SSRM21] (page 885) analyse the current literature on supply chain resilience and muster resilience as a significant topic of current research on supply chains. The outbreak of the COVID-19 pandemic significantly disrupted many global supply chains and shifted a focus on resilience in this area. Shishodia et al. [SSRM21] (page 882) mention one interpretation of resilience as a process of permanent anticipation and reaction to permanent external threats. Furthermore, Shishodia et al. [SSRM21] (page 896) develop the conceptual framework to analyse supply chain resilience as shown in figure 4.4.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

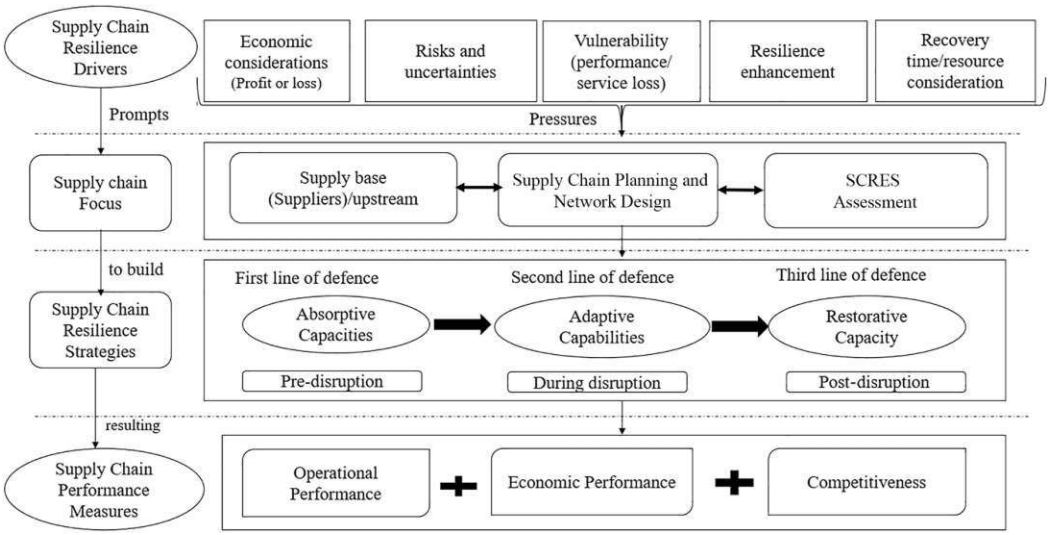


Figure 4.4: Supply Chain Resilience according to Shishodia et al. [SSRM21] (page 896).

4.2.3 Resilience in other Systemic Contexts

Resilience has different meanings in different contexts. As such, it is used in various economic and societal contexts. Resilience describes a desired state of systems that can successfully overcome disruption, stress, trauma or hardship and function under unusual circumstances. It is mentioned in societal contexts such as demographic problems [Dem23] (page 3)and migration systems [Mig23] (recitals 4,5 and 11) across the EU. The term is used in economic contexts such as supply chains [Lor20] (page 244), resilience against foreign subsidies [Res23b] (recital 7), and industrial sectors [Rat23b] (recitals 11 and 12). In his article "Demokratie im Umbruch," Willke refers to the political system of democracy as a resilient political system in its development from Ancient Greece to modern democracies [Wil17] (page 378). The term is also used in the greater context of foreign policy as a resilient society [Rat23a] (recital 4).

4.3 Triad of Resilience: Resistance, Maintaining to Operate & Recovery

Systemic resilience describes a three-part process of initial resistance, the ability to operate under duress within an acceptable quality of service, and the final step of recovering from the impact of a stressful event.

The initial resistance is comparable to the strength of a rock that can tolerate large forces until damage occurs. In psychology, a high initial resistance in an individual is equivalent to a slight stress reaction to a stressful event.

The ability to operate under duress within material science refers to the ability of a structure to create utility during and directly after a stressful event. In psychology, the

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Resistance	Maintaining to Operate	Recovery
2. Close and secure relationships	4. Can deal with whatever comes	1. Able to adapt to change
9. Things happen for a reason	10. Best effort no matter what	7. Coping with stress strengthens
17. Think of self as a strong person	11. You can achieve your goals	8. Tend to bounce back after illness or hardship
19. Can handle unpleasant feelings	12. When things look hopeless, I don't give up	
22. In control of your life	13. Know where to turn for help	
	14. Under pressure, focus and think clearly	
	16. Not easily discouraged by failure	
	20. Have to act on a hunch	

Table 4.1: Sorting the CD-RISC items in the triad of resilience

ability to operate under duress is comparable to that of soldiers to function in battle or escape a dangerous situation.

The last part of recovery in material science can be well demonstrated by a sponge that returns to its original structure after the stress has occurred. In psychology, recovery refers to the ability to minimise the negative impacts after trauma, such as a minimisation of PTSD, depression or anxiety. Recovery in ecological and supply chain resilience can also be characterised by successfully adapting to new circumstances.

The three phases of the triad of resilience are concepts found across all resilience disciplines. Within material science, this triad is visible in the graph 4.2, where the resistance phase starts in the beginning up until $t_{d,i}$. The second phase of maintaining to operate starts at $t_{d,i}$ and ends at $t_{d,f}$. The recovery phase begins at $t_{d,f}$ and ends at T_{ref}. In psychology, the resilience measurements of the CD-RISC can also be roughly categorised into the three phases as in table 4.1.

The items:

3. Sometimes fate or God can help

5. Past success gives confidence for new challenges ı,tem 6. See the humorous side of things

15. Prefer to take the lead in problem-solving

18. Make unpopular or difficult decision

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

21. Strong sense of purpose
23. I like challenges
24. You work to attain your goals
25. Pride in your achievements

fit into more than one of the three phases and were left out of the mapping.

Finally, in cybersecurity, the discipline this master thesis focuses on, the triad of resilience is clearly outlined through different processes. The resistance phase encompasses all preventative measures against stress, such as barriers, firewalls, awareness, encryption, VPNs, segmentation, separation, access control, etc. The second phase of maintaining to operate includes measures such as Business Continuity Management and IT-Service Continuity Management, and the last phase of recovery includes measures such as backup and restore procedures and continual improvement processes.

4.4 Motivation of the DORA

The DORA is one of many laws that the EU set out to release in the greater context of its cybersecurity strategy [EU-20] (pages 4-7) including the NIS2, the Cyber Resilience Act (CRA) and the AI Act. The European Commission formulated 'The EU's Cybersecurity Strategy for the Digital Decade' [EU-20] (page 4), which at its core aims to decrease the European part of the € 5.5 trillion costs (2020) [CCB+20] (page 7) on the global economy caused by cybercrime. It aims to mitigate the systemic risks of cyber attacks on the European population. Especially the interconnection of transportation, energy, health, telecommunications, finance, security, democratic processes, space and defence and the respective sector's dependence on ICT systems and network poses a risk to society comparable to a black swan event. Black swan event, a phrase coined by Taleb [Tal07], describes an event that comes as a surprise with significant effects on systems. The DORA aims to make the financial system more resilient by mandating protection mechanisms and reporting and reducing dependency risks and concentration risks resulting from the use of ICT third-party providers.

In Article 3(1) of the DORA the term "digital operational resilience" is defined as:

"the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions;"

This definition contains several aspects. First, the overall goal of digital operational resilience is operational integrity and reliability. The means to achieve those goals are

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

ICT-related capabilities, more precisely, those ICT-related capabilities needed to provide financial services. The definition contains the information systems that support those services and the connection to the service user in terms of the network in the scope. The definition mentions the minimum threshold as the "services and their quality". Finally, the part "continued provision [...] throughout disruptions" stresses the importance of the second phase of the triad of resilience, ‘maintaining to operate’.

4.5 DORA Audits at the Austrian National Bank

As part of this master thesis, the author interviewed the coordinator of DORA auditing activities of the Austrian National Bank (OeNB) -Stefan Unteregger. The OeNB conducts legal audits of banks in Austria. The key takeaways of this interview are pointed out below. The guiding questions and the complete interview transcript are appended in D.5. Stefan Unteregger agreed with the publication of the transcript, as well as his name and role. The following subsections are inferred and represent the understanding of the appended interview by the author of this thesis. Neither the following sections nor Unteregger’s appended transcript are legally binding advice in any way.

4.5.1 Oversight Frame

As DORA and the surrounding legal norms apply to financial institutions from January 2025 onward, the OeNB is responsible for auditing those legal norms in the banking sector. Due to the OeNB ’s extensive preparation in the area of IT risk over the last decade, no further resources in the form of additional auditors or other personnel are needed to audit DORA on the side of the OeNB.

4.5.2 Changes to current audits

From the perspective of Unteregger, the main impact of DORA is a shift in the legal basis to audit the operational risk stemming from the use of ICT. So far, the legal basis for auditing IT risks in Austria was Paragraph 39 Bankwesengesetz (BWG). This norm mandated banks to manage operational risks adequately. Supervisory IT risk guidelines were based on this relatively short legal construction of Paragraph 39 BWG. DORA introduces its legal basis as a ’level one’ norm and its extension thereof in the form of RTS and ITS as ’level two’ norms. This shift ends any discussions that legal subjects, such as banks, could have started about the adequacy of the EBA guidelines or findings from OeNB audits.

On the other hand, the audits of the OeNB do not change fundamentally under DORA. Neither the scope nor the depth is changing significantly as past audits research a similar level of detail within banks. Similarly, the auditing methods will not change under DORA compared to the status quo.

However, some minor changes are introduced, including the inclusion of ICT third-party providers into the third-party risk management. As of today, ICT third-party providers

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

are not necessarily included in what is currently called 'material outsourcing'. This inclusion of less material ICT third-party providers is one of the examples of an extended scope of OeNB audits under DORA.

Furthermore, DORA contains a clear framework of ICT risk management, which financial institutions can use to ensure operational resilience. Until now, the risk related to outsourcing of ICT and the risks associated with operating ICT were not as well harmonised. However, most obligations exist already for banks.

Whilst the DORA enters into effect on January 2025, financial institutions will not see their cyber-resilience audited instantly. According to Unteregger, the logistical and organisational limitations of the OeNB introduce a time frame, especially for less significant institutions, to finish their implementation efforts after the deadline in time for their first audit under DORA.

4.5.3 External Assurance: Third Party Provider Audits

Regarding certifications for financial institutions and their suppliers, Unteregger commented that standards such as ISO27001 are undoubtedly helpful in showcasing a certain level of cybersecurity. The certifications are, however, not a silver bullet and can not lift obligations to ensure legal requirements are met. This assurance of third-party provider security is one of the critical areas of focus of both DORA and OeNB audits. Financial institutions can use joint audits to ensure their third-party providers comply with contractual and legal obligations. Unteregger further clarifies that big auditing companies might offer such joint auditing services regarding DORA compliance of third-party providers upon which financial institutions can rely.

4.5.4 Focus points of the supervisory authorities

Further, the audits of the OeNB focus on specific topics. Those topics are regularly published by the supervisory authority in close accordance with the Finanzmarktaufsichtsbehörde (FMA). Financial institutions can direct their efforts internally and in auditing third-party providers on those focal points of the supervisory authorities.

4.5.5 Nonconformity in audits

The penalties for non-compliance with legal obligations are manifold. The process starts with findings from audits of the OeNB, which serve initially as a simple notification. As Unteregger mentioned, the bank resolves most findings without further escalating consequences. The auditors know from their experience how long the resolution of findings takes and tolerate resolution time-frames depending on the individual circumstances of the finding and the bank. The inability to resolve findings within a specific time frame further escalates negative consequences ranging from fines to revocation of the banking license.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

4.5.6 Proportionality

Regarding the proportionality principle in Article 4 DORA, Unteregger states that all the requirements introduced by DORA are proportionate because they imply risk adequacy to the financial institution's risk profile. Unteregger emphasises the technology-neutral stance of DORA and the corresponding diversity of implementations that financial institutes can choose from. Unteregger describes further that different business models result in different needs, especially regarding the availability of services. This results in different risk profiles and requirements based on the risk and less on the size of a financial institution. As such, the requirement to implement a SOC and the size of a SOC team is not mandated in DORA for all financial institutions but for those who have a corresponding risk-adequacy. According to Unteregger, this approach ensures proportionality.

4.5.7 Involvement of the OeNB in the legislative procedure

As a competent authority, the OeNB is highly involved in the creation of the legal norms surrounding DORA, from the first drafts of the 'level one' texts up to the latest set of RTS and ITS. Unteregger is personally involved and currently represents the OeNB in a Sub-Committee of the ESA Joint Committee to develop the 'level two' RTS and ITS.

4.5.8 Conclusion of the interview

While DORA does not change the areas or methodology of audits, it does introduce novelty within the topics of audits. It further introduces changes outside of the scope of audits, such as the reporting system under which ICT related incidents and ICT third-party provider relations must be reported to the corresponding authorities.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

CHAPTER 5

Development of a Project Plan Template

5.1 Requirements Engineering

5.1.1 Business Requirements

The business requirements depict the must-haves of the project plan template derived from the literature mentioned above and the review of laws and industry standards. The project plan template must:

- **BR1** cover all aspects of legal norms so that the financial institution's ICT landscape complies with relevant laws after the completion of the project;
- **BR2** align the internal governance with the actual state of the ICT assets and processes.
- **BR3** aim for a state-of-the-art ICT landscape of management, IT controls and technical implementation.
- **BR4** mitigate the top threats relevant for financial institutions.

5.1.2 Functional Requirements

The functional requirements are derived from the business requirements and provide details on the required contents of the project plan template.

The project plan template must:

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

- **FR1** Formulate the ICT strategy, the Information Security Strategy, list the internal resources required for ICT and Information Security, the roles & responsibilities regarding ICT and information security and implement the Information Security Management System;
- **FR2** Include the ICT risk management, the project management, the internal control and the 3 lines of defence model;
- **FR3** Formulate the information security policy for the Human Ressources (HR) department;
- **FR4** Align the third party/supplier management with the state of the art and in compliance with DORA;
- **FR5** Entail the facility management and ensure the management of physical security;
- **FR6** Ensure the collection, protection and processing of personal data in compliance with the GDPR;
- **FR7** Align the entire reporting system regarding ICT related incidents with supervisory requirements;
- **FR8** Entail the compliance with contractual & legal requirements regarding information security
- **FR9** define and implement the security-related processes regarding Vulnerability Management, Incident Management, BCM and IT Service Continuity Management (ITSCM);
- **FR10** Define and implement the processes regarding the modification of the ICT landscape including: Change Management, Patch-& Release Management and Requirements Management;
- **FR10** Ensure the adequacy of its Threat Intelligence, Anti Fraud Management, Functional & Security Testing, Backup Management, Crisis Communication, Restore & Recovery Planning and Emergency Exercises & Tests;
- **FR11** Ensure the application of the IT Security Concepts regarding Cryptography & Key Management, Strong Authentication, Secure Data Processing & Transmission, Secure Data Erasure and Disposal and the application of an entity-wide Secure Configuration Baseline for ICT systems;
- **FR12** Define and implement the IT operations processes, including IT Operations Management, Configuration Management, Asset Management, Availability Management and Mobile Device Management;
- **FR13** Ensure a secure IT Infrastructure setup;

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

- **FR14** Ensure the setup of the technical monitoring of the ICT assets such as data, clients and systems;
- **FR15** Ensure the adequacy and documentation of the facility security;

Furthermore, the graphic 3.3 provides a structured overview of the areas that must be reviewed and adapted where necessary. More detailed requirements for each area of influence are not listed as it would go beyond the scope of this thesis to list all requirements of each area.

5.1.3 Non Functional Requirements

The non-functional requirements depict the requirements that ensure that the project plan format has a high degree of usability and value to practitioners.

To fulfil the non-functional goals, the project plan template must:

- **NFR1** Be easy to grasp and include a high-level overview of the project;
- **NFR2** Demonstrate a high degree of applicability and correspondingly suffices with minimal additional customisation;
- **NFR3** Demonstrate its applicability as a guiding document across project phases;
- **NFR4** Indicate an order and dependencies of individual work packages;
- **NFR5** Contain relevant success metrics;
- **NFR6** Enumerate key stakeholder;
- **NFR7** Outline deliverables;
- **NFR8** Develop actionable tasks;
- **NFR9** Assign tasks and deadlines;
- **NFR10** Identify relevant project risks and effective treatments;

5.2 Design and Creation of the Project Plan Template

This section outlines the creation process of the project plan template.

The project plan template is created in two parts. The first part sets the project frame. The literature requirements are formulated into concrete items and added to the frame. They are validated along with the requirements during the creation. The second part of the project plan template consists of the three areas of working packages, namely organisational governance/management, IT controls and technical implementation. The working packages are derived from the meta-synthesis as in figure 3.3. The description is

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

added with resources from the literature. The necessary inputs per package are derived from the author's analysis of the contents of each work package. The objectives are derived from the legal requirements in the DORA and the surrounding level two texts.

The focus of the project plan template is to be used as a guide and as an overview over ICT compliance projects. As such, it does not need to provide detailed step-by-step instructions, but it refers to other documents such as industry standards and legal norms or states a work package frame. The entire project plan template is enclosed in the Annex.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

CHAPTER 6

Design Verification against Requirements

This chapter outlines the extent to which the artifact meets requirements, thereby mitigating the risks of legal noncompliance and cyber threats.

6.1 Legal Verification

The verification of legal requirements is approximated by enumerating all paragraphs of the DORA and listing all related working packages from the plan B that cover the corresponding part of DORA.

6.1.1 DORA

Article 1: Subject Matter This Article describes the subject matter of the norm; no concrete obligations for financial entities result.

Article 2: Scope This Article is an enumeration of different financial entities in this regulation's scope; no obligations for financial entities result.

Article 3: Definitions This Article only contains word definitions. No obligations result.

Article 4: Proportionality principle This Article explains how the rules laid out for financial entities are to be applied. No obligations result.

Article 5: Governance and organisation B.1.4, B.1.7, B.1.12

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Article 6: ICT risk management framework B.1.1, B. 1.2,B.1.5, B.1.6, B.1.7, B.1.12, B.1.18

Article 7: ICT systems, protocols and tools B.1.9

Article 8: Identification B.1.2, B.1.3, B.1.6, B.1.14, B.2.4, B.2.8, B.2.1, B.2.20

Article 9: Protection and prevention B.1.9, B.2.15, B.2.16, B.2.20, B.2.21, B.2.25, B.3.3

Article 10: Detection B.1.4, B.2.14, B.3.7

Article 11: Response and Recovery B.1.6, B.1.17, B.1.18, B.2.2, B.2.10, B.2.11

Article 12: Backup policies and procedures, restoration and recovery procedures and methods B.2.3, B.2.5, B.2.11

Article 13: Learning and evolving B.1.2, B.1.3, B.1.4, B.1.6, B.1.9, B.1.12, B.2.9

Article 14: Communication B.1.7, B.2.12, B.2.14

Article 15: Further harmonisation of ICT risk management tools, methods, processes and policies This Article is strictly directed at the ESA regarding RTS. No obligations for financial entities result.

Article 16: Simplified ICT risk management framework This paragraph only targets a subset of small financial institutions. It is a subset of the other obligations. It is excluded from this thesis as described in the limitations; see 9.3.

Article 17: ICT-related incident management process B.2.9

Article 18: Classification of ICT-related incidents and cyber threats B.2.9

Article 19: Reporting of major ICT-related incidents and voluntary notification of significant cyber threats B.1.18, B.2.9, B.2.12

Article 20: Harmonisation of reporting content and templates This Article is directed at the ESA to implement RTS and ITS

Article 21: Centralisation of reporting of major ICT-related incidents This Article is directed at the ESA to expand the centralisation of incident reporting.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Article 22: Supervisory feedback This Article is directed at competent authorities and the ESA regarding feedback on incident notifications.

Article 23: Operational or security payment-related incidents concerning credit institutions, payment institutions, account information service providers, and electronic money institutions This Article subjects additional organisations, as listed in the title, to the obligations in Articles 17 to 22. No additional obligations result.

Article 24: General requirements for the performance of digital operational resilience testing B.2.2

Article 25: Testing of ICT tools and systems B.2.2

Article 26: Advanced testing of ICT tools, systems and processes based on Bankwesengesetz (TLPT) This Article is only directed at a small subset of financial institutions that qualify for TLPT. It is excluded from this thesis as described in the limitations; see 9.3.

Article 27: Requirements for testers for the carrying out of TLPT This Article is only directed at a small subset of financial institutions that qualify for TLPT. It is excluded from this thesis as described in the limitations; see 9.3.

Article 28: General principles B.1.13, B.1.14, B.1.15, B.1.17, B.1.18, B.2.10

Article 29: Preliminary assessment of ICT concentration risk at entity level B.1.16, B.1.19

Article 30: Key contractual provisions B.1.16

Article 31: Designation of critical ICT third-party service providers This Article is directed at the ESA to designate certain ICT third-party providers. No obligations for financial entities result.

Article 32: Structure of the Oversight Framework This Article describes establishing a new authority. No obligations for financial entities result.

Article 33: Tasks of the Lead Overseer This Article describes the tasks of a public authority. No obligations result from financial entities.

Article 34: Operational coordination between Lead Overseers The same limitations as in Article 33 apply.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Article 35: Powers of the Lead Overseer The same limitations as in Article 33 apply.

Article 36: Exercise of the powers of the Lead Overseer outside the Union The same limitations as in Article 33 apply.

Article 37: Request for information The same limitations as in Article 33 apply.

Article 38: General investigations The same limitations as in Article 33 apply.

Article 39: Inspections The same limitations as in Article 33 apply.

Article 40: Ongoing oversight The same limitations as in Article 33 apply.

Article 41: Harmonisation of conditions enabling the conduct of the oversight activities This Article is directed at the ESA regarding RTS.

Article 42: Follow-up by competent authorities This Article describes the consequences for ICT third-party providers. No obligations for financial entities result.

Article 43: Oversight fees This Article regulates the fees for oversight. No obligations result.

Article 44: International cooperation This Article strictly addresses the authorities. No obligations result.

Article 45: Information-sharing arrangements on cyber threat information and intelligence This Article provides an optional involvement of financial entities in information-sharing arrangements. No obligations result.

Article 46: Competent authorities This Article designates competent authorities for each financial institution. No obligations result.

Article 47: Cooperation with structures and authorities established by Directive (EU) 2022/2555 This Article describes possible cooperation between authorities. No obligations result.

Article 48: Cooperation between authorities This Article describes the cooperation between authorities. No obligations result.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Article 49: Financial cross-sector exercises, communication and cooperation This Article describes the internal works of the ESA. No obligations for financial entities result.

Article 50: Administrative penalties and remedial measures This Article describes the minimum penalties member states have to provide for competent authorities. No obligations result for financial entities.

Article 51: Exercise of the power to impose administrative penalties and remedial measures This Article describes how penalties may be applied. No obligations result.

Article 52: Criminal penalties This Article describes how the member states must handle criminal penalties. No obligations result.

Article 53: Notification duties This Article describes the reporting duties of member states. No obligations for financial entities result.

Article 54: Publication of administrative penalties This Article describes how penalties of competent authorities must be publicised. No obligations for financial entities result.

Article 55: Professional secrecy This Article describes how competent authorities handle information. No obligations for financial entities result.

Article 56: Data Protection This Article regulates the personal data handling of the authorities. No obligations for financial entities result.

Article 57: Exercise of the delegation This Article describes the law making process. No obligations for financial entities result.

Article 58: Review clause This Article describes a review of the DORA by 2026 and 2028. No obligations for financial entities result.

Article 59: Amendments to Regulation (EC) No 1060/2009 This Article changes a regulation regarding credit rating agencies by inserting a reference to the DORA. No additional obligations for financial entities result.

Article 60: Amendments to Regulation (EU) No 648/2012 This Article changes a regulation regarding central counterparts by referencing the DORA. It is excluded from this thesis as described in the limitations; see 9.3.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Article 61: Amendments to Regulation (EU) No 909/2014 This Article changes a regulation regarding central security depositories. It is excluded from this thesis as described in the limitations; see 9.3.

Article 62: Amendments to Regulation (EU) No 600/2014 This Article inserts references to the DORA into a regulation. No obligations for financial entities result.

Article 63: Amendment to Regulation (EU) 2016/1011 This Article changes a regulation regarding benchmarks and performance measurements by referencing the DORA.

Article 64: Entry into force and application This Article sets the time frames for the regulation to enter into force. No obligations for financial entities result.

6.1.2 Consultation paper on draft RTS ICT risk management tools methods processes and policies

Article 1: General elements of ICT security B.1.1, B.1.9

Article 2: Provisions on governance B.1.5, B.2.15

Article 3: ICT risk management B.1.2, B.1.3, B.1.6, B.2.10

Article 4: ICT asset management policy B.2.1

Article 5: ICT asset management procedure B.2.1

Article 6: Encryption and cryptographic controls B.2.15

Article 7: Cryptographic key management B.2.16

Article 8: ICT operating policies and procedures B.2.3

Article 9: Capacity and performance management B.2.5

Article 10: Vulnerability and patch management B.2.7, B.2.21

Article 11: Data and system security B.2.4, B.2.6, B.2.18, B.2.19, B.2.24, B.2.25, B.3.4, B.3.5

Article 12: Logging B.3.6

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Article 13: Network security management B.2.19, B.3.2, B.3.3

Article 14: Securing information in transit B.2.15, B.3.4

Article 15: ICT project management B.1.8

Article 16: ICT systems acquisition, development, and maintenance B.2.2, B.2.22, B.2.23

Article 17: ICT change management B.2.20

Article 18: Physical and environmental security B.3.1, B.3.8

Article 19: ICT and information security awareness and training B.1.12

Article 20: Human resources policy B.1.10, B.1.11, B.1.12

Article 21: Identity management B.2.24

Article 22: Access control B.1.5, B.2.17, B.2.25, B.3.1, B.3.8

Article 23: ICT-related incident management policy B.2.9

Article 24: Anomalous activities detection and criteria for ICT-related incidents detection and response B.1.11, B.2.8, B.2.9, B.3.7

Article 25: Components of the ICT business continuity policy B.2.10

Article 26: Testing of the ICT business continuity plans B.2.14

Article 27: ICT response and recovery plans B.2.11, B.2.13

Article 28: Format and content B.1.9, B.1.18

Article 29: Complexity and risk considerations This Article describes how the obligations will be implemented. No additional obligations for financial entities result.

Article 30: Governance and organisation This Article deals with the simplified risk management framework. It is excluded from this thesis as described in 9.3.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Article 31: Information security policy and measures This Article deals with the simplified risk management framework. It is excluded from this thesis as described in 9.3.

Article 32: Classification of information assets and ICT assets This Article deals with the simplified risk management framework. It is excluded from this thesis as described in 9.3.

Article 33: ICT risk management This Article deals with the simplified risk management framework. It is excluded from this thesis as described in 9.3.

Article 34: Physical and environmental security This Article deals with the simplified risk management framework. It is excluded from this thesis as described in 9.3.

Article 35: Access Control This Article deals with the simplified risk management framework. It is excluded from this thesis as described in 9.3.

Article 36: ICT operations security This Article deals with the simplified risk management framework. It is excluded from this thesis as described in 9.3.

Article 37: Data, System and Network Security This Article deals with the simplified risk management framework. It is excluded from this thesis as described in 9.3.

Article 38: ICT security testing This Article deals with the simplified risk management framework. It is excluded from this thesis as described in 9.3.

Article 39: ICT systems acquisition, development, and maintenance This Article deals with the simplified risk management framework. It is excluded from this thesis as described in 9.3.

Article 40: ICT project and change management This Article deals with the simplified risk management framework. It is excluded from this thesis as described in 9.3.

Article 41: Components of the ICT business continuity plan This Article deals with the simplified risk management framework. It is excluded from this thesis as described in 9.3.

Article 42: Testing of business continuity plans This Article deals with the simplified risk management framework. It is excluded from this thesis as described in 9.3.

Article 43: Format and content This Article deals with the simplified risk management framework. It is excluded from this thesis as described in 9.3.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

6.1.3 Consultation paper on draft RTS on classification of ICT incidents

This draft RTS details how incidents must be classified. These classification details must be noted during the work package B.2.9

6.1.4 Consultation paper on draft ITS on register of information

This draft ITS describes in detail how the register of information regarding ICT third-party provider must be submitted. This standard must be implemented during the work package B.1.18.

6.1.5 Consultation paper on draft RTS on policy on the use of ICT services regarding critical and important functions

Article 1: Complexity and risk considerations B.1.13, B.1.15

Article 2: Group application B.1.15

Article 3: Governance arrangements regarding the policy on the use of ICT services supporting critical or important functions B.1.6, B.1.13, B.1.15, B.1.16

Article 4: ICT third-party service providers and ICT services supporting critical or important functions B.1.13

Article 5: Main phases of the life cycle for the use of ICT services supporting critical or important functions provided by ICT third-party service providers B.1.13

Article 6: Ex-ante risk assessment B.1.13, B.1.15

Article 7: Due diligence B.1.13, B.1.15

Article 8: Conflict of interest B.1.13

Article 9: Contractual clauses for the use of ICT services supporting critical or important functions B.1.16

Article 10: Monitoring of the contractual arrangements for the use of ICT services supporting critical or important functions B.1.16

Article 11: Exit and termination of contractual arrangements for the use of ICT services supporting critical or important functions B.1.17

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Article 12: Entry into force Not applicable.

6.1.6 Results of the legal verification of requirements

The project plan template covers all relevant Articles of the DORA and the corresponding RTS and ITS that are inside the scope of this thesis (for limitations, see 9.3), with at least one working package per Article. The table 6.1 sums up the Articles that are relevant for financial institutions, the project plan template and, whether they were covered by working packages in the project plan template and, if so, by how many working packages.

Amount of working packages in chapter B covering the Article	Amount of Articles (DORA)	Amount of Articles (RTS on risk management)	Amount of Articles (RTS on C&I functions)
Not relevant for FI	35	0	0
No obligations for FI	6	1	1
Excluded as a limitation (See 9.3)	5	14	0
0	0	0	0
1	6	14	7
2	1	7	3
3	5	3	0
4	0	2	1
5+	6	2	0

Table 6.1: Coverage of Articles in the DORA and related RTS within the project plan template. Source: Created by the author.

Table 6.2 describes metrics to measure the relative coverage of the Articles in the DORA and the enclosed RTS rounded to the nearest percentage point. Amongst Articles relevant to financial institutions, containing obligations for financial institutions and are in this thesis' scope, all Articles (100%) are covered by working packages in the project plan template in section B.

Not mentioned in the tables 6.1 and 6.2 are the RTS on the classification of ICT incidents and the ITS on the register of information. Those are covered by one working package each.

6.2 Technical Verification

To evaluate the project plan against industry standards, the ISO27001:2022 and its Annex (A) are compared to the project plan template in a similar fashion as in the section above with the DORA. The leading number refers to the chapters of the ISO27001 and the control of the Annex of ISO27001.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Performance indicator	DORA	RTS on risk management	RTS on C&I functions
Total coverage of all Articles	28%	65%	92%
Coverage of all Articles relevant for FI	62%	65%	92%
Coverage of the relevant Articles with obligations	78%	67%	100%
Coverage of the relevant Articles with obligations in scope (See 9.3)	100%	100%	100%

Table 6.2: Percentage of Articles covered by working packages in the project plan template. Source: Created by the author.

1 Scope: This chapter summarises the norm's scope. No tasks result.

2 Normative references: This chapter describes the structure. No task result.

3 Terms and definitions: This chapter defines terms. No tasks result.

4.1 Understanding the organization and its context: B.1.2

4.2 Understanding the needs and expectations of interested parties: B.1.1

4.3 Determining the scope of the information security management system: B.1.9

4.4 Information security management system: B.1.9

5.1 Leadership and commitment: B.1.9

5.2 Policy: B.1.1, B.1.9

5.3 Organizational roles, responsibilities and authorities: B.1.5, B.1.6, B.1.7, B.1.11

6.1 Actions to address risks and opportunities: B.1.3

6.2 Information security objectives and planning to achieve them: B.1.3, B.1.9

7.1 Resources: B.1.4

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

7.2 Competence: B.1.7, B.1.11, B.1.12

7.3 Awareness: B.1.10, B.1.12

7.4 Communication: B.1.9

7.5 Documented information: B.1.2, B.1.5, B.1.6, B.1.11

8.1 Operational planning and control: B.1.9, B.2.3

8.2 Information security risk assessment: B.1.2, B1.3, B.1.15

8.3 Information security risk treatment: B.1.3, B.1.15

9.1 Monitoring, measurement, analysis and evaluation: B.1.3, B.2.14

9.2 Internal audit: B.1.5, B.1.6

9.3 Management review: B.1.6

10.1 Continual improvement: B.1.6, B.1.9, B.1.12, B.2.14

10.2 Nonconformity and corrective action: B.1.6, B.1.9

The following enumeration regards the controls as listed in the Annex of ISO27001. The leading number (e.g. A5.1) refers to the number of the control as enumerated in the Annex of ISO27001.

A5.1 Policies for information security: B.1.1, B.1.9

A5.2 Information security roles and responsibilities: B.1.5, , B.1.6, B.1.7, B.1.11

A5.3 Segregation of duties: B.1.5, B.1.7, B.1.11

A5.4 Management responsibilities: B.1.5, B.1.7, B.1.11

A5.5 Contact with authorities: B.1.18

A5.6 Contact with special interest groups: Not included.

A5.7 Threat intelligence: B.2.8

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

A5.8 Information security in project management: B.1.8

A5.9 Inventory of information and other associated assets: B.2.1

A5.10 Acceptable use of information and other associated assets: B.1.9

A5.11 Return of assets: B.1.12

A5.12 Classification of information: B.2.1

A5.13 Labelling of information: B.2.1

A5.14 Information transfer: B.2.15

A5.15 Access control: B.2.25

A5.16 Identity management: B.2.24

A5.17 Authentication information: B.2.17

A5.18 Access rights: B.2.25

A5.19 Information security in supplier relationships: B.1.15

A5.20 Addressing information security within supplier agreements: B.1.16, B.1.17

A5.21 Managing information security in the information and communication technology (ICT) supply chain: B.1.13, B.1.14, B.1.15

A5.22 Monitoring, review and change of management of supplier services: B.1.13, B.1.14

A5.23 Information security for use of cloud services: Not included.

A5.24 Information security incident management planning and preparation: B.2.9, B.2.12

A5.25 Assessment and decision on information security events: B.2.9

A5.26 Response to information security incidents: B.2.9, B.2.12

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

A5.27 Learning from information security incidents: B.2.9

A5.28 Collection of evidence: B.2.9

A5.29 Information security during disruption: B.2.10, B.2.12

A5.30 ICT readiness for business continuity: B.2.10

A5.31 Legal statutory, regulatory and contractual requirements: B.1.18

A5.32 Intellectual property rights: Not included.

A5.33 Protection of records: B.2.11, B.2.13, B.2.15

A5.34 Privacy and protection of personally identifiable information (PII): B.1.19

A5.35 Independent review of information security: B.1.9

A5.36 Compliance with policies, rules and standards for information security: B.1.9

A5.37 Documented operating procedures: B.2.3, B.2.13

A6.1 Screening : B.1.10

A6.2 Terms and conditions of employment: B.1.10

A6.3 Information security awareness, education and training: B.1.12

A6.4 Disciplinary process: B.1.9

A6.5 Responsibilities after termination or change of employment: B.1.10

A6.6 Confidentiality or non-disclosure agreements : B.1.10

A6.7 Remote working: B.1.9

A6.8 Information security event reporting : B.1.9

A7.1 Physical security perimeter: B.3.1, B.3.8

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

A7.2 Physical entry controls: B.3.1, B.3.8

A7.3 Securing offices, rooms and facilities: B.3.1, B.3.8

A7.4 Physical security monitoring: B.3.8

A7.5 Protecting against physical and environmental threats: B.3.1, B.3.8

A7.6 Working in secure areas: B.3.8

A7.7 Clear desk and clear screen: B.1.9

A7.8 Equipment siting and protection: B.3.8

A7.9 Security of assets off-premises: B.3.8

A7.10 Storage media: B.1.9, B.2.15

A7.11 Supporting utilities: Not included.

A7.12 Cabling security: B.3.2

A7.13 Equipment maintenance: B.2.3

A7.14 Secure disposal or re-use of equipment : B.2.18

A8.1 User endpoint devices: B.2.6

A8.2 Privileged access rights: Not included.

A8.3 Information access restriction: B.2.25

A8.4 Access to source code: B.2.22

A8.5 Secure authentication: B.2.17

A8.6 Capacity management : B.2.5

A8.7 Protection against malware : B.3.5

A8.8 Management of technical vulnerabilities: B.2.7

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

A8.9 Configuration management: B.2.4, B.2.19

A8.10 Information deletion: B.2.18

A8.11 Data masking: Not included

A8.12 Data leakage prevention: B.3.4

A8.13 Information backup: B.2.11, B.2.13

A8.14 Redundancy of information processing facilities : B.2.11

A8.15 Logging: B.3.6

A8.16 Monitoring activities: B.3.7

A8.17 Clock synchronization: Not included

A8.18 Use of privileged utility programs: B.3.5

A8.19 Installation of software on operational systems: B.2.6

A8.20 Network controls: B.3.2

A8.21 Security of network services: B.2.15, B.3.2

A8.22 Segregation in networks: B.3.3

A8.23 Web filtering: B.3.2

A8.24 Use of cryptography: B.2.15, B.2.16

A8.25 Secure development lifecycle: B.2.22

A8.26 Application security requirements: B.2.13, B.2.19

A8.27 Secure system architecture and engineering principles: B.2.23

A8.28 Secure coding: B.2.2, B.2.21, B.2.22

A8.29 Security testing in development and acceptance: B.2.2

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

A8.30 Outsourced development: B.2.23

A8.31 Separation of development, test and production environments: B.2.2, B.2.21

A8.32 Change management: B.2.20, B.2.22

A8.33 Test information: B.2.2

A8.34 Protection of information systems during audit and testing: B.2.2

6.2.1 Results of the technical verification of requirements

The project plan template covers all relevant chapters of the ISO27001 norm and 92% of the controls in the Annex of the ISO27001 norm with at least one working package per chapter and control. The following table 6.3 summarises the coverage of chapters and controls by working packages within the project plan.

Amount of working packages in chapter B covering one ISO control	Amount of controls (ISO27001)	Amount of controls (Annex)
Not relevant for FI	0	0
No obligations for FI	3	0
Excluded as a limitation (See 9.3)	0	0
0	0	7
1	9	61
2	8	19
3	1	5
4	3	1
5+	0	0

Table 6.3: Coverage of controls from the ISO27001 within the project plan template. Source: Created by the author.

The following items were listed as control in the Annex of ISO27001 but were not mapped within the project plan template:

- A5.6 Contact with special interest groups
- A5.23 Information security for use of cloud services
- A5.32 Intellectual property rights

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Performance indicator	ISO27001	Annex
Total coverage of all chapter/controls	88%	92%
Coverage of all chapters/controls relevant for FI	88%	92%
Coverage of the relevant chapter/controls with obligations	100%	92%
Coverage of the relevant chapter/controls with obligations in scope (See 9.3)	100%	92%

Table 6.4: Percentage of chapters/controls covered by working packages in the project plan template. Source: Created by the author.

- A7.11 Supporting utilities
- A8.2 Privileged access rights
- A8.11 Data masking
- A8.17 Clock synchronization

The table 6.4 describes metrics to measure the relative coverage per chapter and control of the ISO27001 by at least one working package in the project plan template rounded to the neared percentage point.

6.3 Threats mapping to Working Packages

As listed in chapter 1.1.1, the following threats are the most common cyber threats faced by organisations in 2023.

- Ransomware
- Malware
- Social engineering
- Threats against data
- Threats against availability: Denial of Service
- Threat against availability: Internet threats

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Threat	Working Package
Ransomware	B.1.19, B.2.3, B.2.11, B.2.13, B.3.3, B.3.6
Malware	B.2.15, B.3.3, B.3.5
Social engineering	B1.12
Threats against data	B.1.19, B.2.4, B.2.15, B.2.16 B.2.18, B.2.19, B.3.4
Threats against availability: Denial of Service	B.2.5, B.2.13, B.3.2
Threat against availability: Internet threats	B.2.5, B.3.2
Information manipulation and interference	
Supply chain attacks	B.1.8, B.2.21, B.2.22, B.2.23

Table 6.5: Mapping of working packages that directly mitigate the corresponding top threat. Source: Created by the author.

- Information manipulation and interference
- Supply chain attacks

Similarly to the two sections above, the working packages in the project plan template are mapped onto those identified top threats to organisations to demonstrate risk mitigation in table 6.5. Additionally, to work packages that can be directly mapped on a threat, many measures mitigate the general risk and impact of cyber threats, such as ICT risk management, emergency exercises, incident management or business continuity management. This project plan template does not cover the threat of information manipulation and interference.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

CHAPTER 7

Qualitative Evaluation through Expert Interviews

7.1 Selection of Experts

The selection of interview partners is conducted through the author's network. CISOs and persons with comparable positions within financial institutions or persons with a long record of compliance and ICT-related projects are considered experts. The following experts are recruited.

DI Markus Endres: Markus Endres is managing partner at Certitude Consulting GmbH. CertITude is a consulting firm specialising in managing information and communication technology risks. He holds the role as CISO in several Austrian banks. Before his partnership at CertITude, he worked in various positions in the banking sector, including Chief Risk Officer at Semper Constantia Privatbank AG, Senior Manager at zeb consulting - a Finance and Risk Consultancy -, Senior Manager at PwC Austria and as a referent for the banking revision for significant institutions at the OeNB. His professional experience revolves around IT Risk Management and Information Security.

Markus Hefler: Markus Hefler is currently the CISO of the Raiffeisen-Landesbank Steiermark and former CISO of the Raiffeisen Informatik Center Steiermark GmbH. He worked the last 15 years as a CISO in the financial sector, first for an ICT third-party provider, then for a bank. His expertise in the information security domain is further exemplified through his acquisition of certifications such as CISSP, CISM, CISA, CDXP, and CDPSE. Besides his professional career, he is pursuing a Master of Business Administration at the Johannes Kepler University Linz.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Michael Clauss: Michael Clauss is currently the head of regulatory compliance at Airbus Defence and Space. In the past twenty years, he has held various positions within the Airbus Group, ranging from project manager to financial controller, enterprise risk manager, and regulatory compliance manager. His projects relate to aviation, space, defence and communication solutions, including cybersecurity-related projects and requirements. His current responsibilities include product-related legal and contractual compliance. His academic background includes a master of business administration, a master of science in engineering, and a diploma in engineering from TU Berlin. He is certified as a Project Management Professional (PMP) of the Project Management Institute (PMI).

7.2 Conducting Expert Interviews

The interviews are conducted through the following process:

Preparation: The interviewees are informally contacted regarding their interest in participating in this master thesis as experts through verbal approach and e-mail. Upon signalled interest, the interviewees receive the documents describing the interview process as in A and the document including the project plan template as in B. Then, the interviews are scheduled.

Conduction: At first, the purpose of the interview is explained. Then, the interviewees are asked for consent to record the interview, and the extent of their involvement and the planned publication intentions are explained. Next, the format of the interview is presented and after that, the interview begins. The interviewees are guided through the interview questions. However, the interviewer has the liberty to stray from the questions if a question is already answered or an answer induces further questions or statements of clarification. Questions from the interviewees are also responded swiftly. During the evaluation of the project plan template, the interviewees have the additional chance to review the documents together with explanations from the interviewer.

Finalisation After the interviews are conducted, the interviewees receive the transcript of the interview and the possibility to amend any statements and redact their name or association with any organisation within 14 days.

7.3 Interview Data Analysis Methods

7.3.1 Recording

The interviews are recorded using the author's smartphone recording function. The recordings are retained in the author's archive and are not further disclosed following the confidentiality agreement with the interviewees.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

7.3.2 Transcription

The audio recordings are initially analysed using the online application riverside.fm. They are then checked for unity with the recordings using manual transcription. Ylvali Koch and Konstantin Denzel support the author in the manual transcription. The author finally checks all transcripts for unity with the tapes. The interviews are held in German. However, interviewees use some level of dialect, which is translated into Standard German during the manual transcription process. All transcripts are reviewed by the corresponding interviewee based on the original statements and intentions. The interviewees used the possibility to clarify and edit their answers.

7.4 Results

7.4.1 Question on overview of professional background experience in ICT-related project management

The first question is answered diversely according to the experience of each interviewee. All interviewees have a highly professional background and a decade-long experience managing ICT projects and information security. One expert has a strong background in regulatory compliance projects, partly in cyber-resilience and communication. All interviewees show an extensive background of working with laws and standards of information security.

7.4.2 Question on key elements for an effective project plan

The second question regarding key elements of an effective project plan is answered with different enumerations of essential items for successful project planning. One element mentioned in the interviews is the definition of project goals and project non-goals in communicating with all relevant stakeholders. Additionally, naming the sponsors and ensuring their support is mentioned by one interviewee. Another element is the communication of stakeholders regarding their expectations towards this project. Other elements mentioned are defined outcomes of working packages, needed resources, timelines and deadlines. Further, a clear structure for the project is mentioned as an essential part. Within a clear structure, relations between working packages, critical paths and a realistic time plan were mentioned.

7.4.3 Question on valuable section or aspect of the project plan template

All sections are deemed helpful or strictly required when asked about valuable sections or aspects. Helpful sections include the KPI, the project risks and mitigation strategies. Required sections include the frame and the work package enumeration. Two interviewees highlight the importance of third-party risk management regarding DORA. This area will surprise many organisations since the EBA outsourcing guidelines are comparably young

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

and not yet as well established. Further, the connected issue of contract management and the inclusion of standard contract clauses are deemed essential since these working packages are very intense and, in many organisations, they do not get as much focus as needed.

7.4.4 Question on ease of understanding the format and the content

According to all interviewees, the project plan template format is easy to understand and well-chosen. One interviewee points out that this template can serve as a basis for a project plan and is exceptionally well-suited for project documentation. Further, the format makes it easy to evaluate the document and append it as an academic result. For practitioners, the format is valuable enough to be used as a basis to develop individual project plans further, like an instruction set.

7.4.5 Question on sensible choice of document format

Whether or not the format is chosen sensibly induces further questions from all interviewees. According to the interviewees, the choice of format is well suited for project documentation, as a guideline to instantiate a concrete project plan for academic evaluation and as an academic artefact. However, the format is not as well suited to be used directly in a project as it lacks content, i.e., a complete definition of work packages, dependency analysis such as critical paths and a graphical overview of the current status.

For the format to be used in practice, it must be further transformed according to each organisation's circumstances and requirements. It is, however, helpful as a guide or base for a project plan. More details are needed then to define work packages according to best practices. Furthermore, tracking projects over time is not well facilitated with the artefact as it is.

7.4.6 Question on suggestion for other formats

When asked about possible other formats, the interviewees suggested using project planning tools or an advanced Excel tool. Those are more used in practice than a LaTeX/PDF document such as the current artefact.

7.4.7 Question on a clear definition of the implementation steps and objectives

This question divides the interviewees as one states that the definition of the work packages provides enough details to derive the implementation steps and objectives. Another states that - as it is - the working packages do not provide the detail needed to start with the implementation steps directly. Still, it is enough to give an overview and start with a further definition of each work package because the current suggested clustering is well enough structured to dive into a work package and define it further. However, more planning and defining must be undertaken as part of a project planning

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

phase to start with a work package. According to the interviewee, further planning could be provided as part of this abstract template.

7.4.8 Question on ease of understanding, usefulness and ease of measurability of KPI

The interviewees uniformly state that the set of provided KPI is easy to understand. One interviewee notes that the KPI regarding team members joining and leaving the team is not helpful. Otherwise, all interviewees agree that the KPIs are helpful for project control and management. The measurability of all KPIs is noted as highly dependent on the available data, the project and the organisation. One interviewee notes that time tracking is hard to implement in organisations where employees do not regularly track their time on individual activities.

Two interviewees suggest that an additional KPI would be beneficial. This additional KPI should reflect the completion percentage of the project. One such KPI could be the percentage of completed work packages. A more fine-grained KPI could be the approach to adding partially finished working packages to the aggregated completion percentage. Even more fine-grained would be a KPI that would incorporate a weight-based completion of work package that weighs the estimated effort per work package into the completion percentage. Another KPI, an interviewee suggested and linked to the concept of on-time completion percentage, is milestone adherence.

7.4.9 Question on clear overview and guide to implement cyber-resilience

The interviewees agree that the project plan template provides a clear overview of cyber-resilience projects. They further agree that the document provides a helpful guide for cyber-resilience projects. One interviewee pointed out that the template can be a helpful starting point and guideline to implement and document organisations' DORA compliance.

7.4.10 Question on the relevance of the project risks

The interviewees agreed that the listed project risks are highly relevant. All interviewees encountered the listed project risks during their professional careers. The interviewees suggest some fine-tuning of the existing project risks. The risk related to Resistance to Change depends highly on the organisational culture and stance on agile structures versus traditional structures. Further, the Resistance to Change depends on how solid processes and particular mindsets are established. Another fine-tuning of project risks to the risk associated with the Scarcity of Project Resources is the lack of financial or technical resources. This addition expands the current project risk from only focusing on the scarcity of personnel.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Further, some additional project risks are mentioned by the interviewees. One such risk is a lack of specific knowledge in the organisation regarding technical cybersecurity, BCM, ICT risk management or third-party risk management. Another additional DORA related risk is a change in the legislature since there might still be additions from the current interpretation through a change in the final RTS and ITS. Therefore, starting prematurely with DORA related projects could risk necessary changes. The last additional project risk mentioned by an interviewee is the dependency towards third parties such as central ICT third-party providers, as they play a central role in DORA related requirements but are not under the direct influence of the financial institution. Finally, one interviewee pointed out that cyber-resilience projects are cross-organisational and require a robust decision process along the project implementation.

7.4.11 Question on the correctness and usefulness of risk mitigation strategies

The risk mitigation strategies are deemed helpful by the interviewees. Some strategies are commented such as the strategy on resistance to change, where one interviewee added that prioritising the project would not work in the expert's current organisation. However, a helpful mitigation strategy would be a commitment from the complete top-level management.

Another interviewee added that the strategy against scarcity of project resources should also include close project tracking and reporting to ensure the availability of resources throughout the implementation of the project. This continuous involvement and information for the management could aid in ensuring management buy-in and management commitment throughout the project. Further, the commitment of each project team member to fulfil their part during meetings could improve ensuring work is done.

The second risk mitigation strategy against a gap between documentation and implementation should include internal resources and the relevant personnel to ensure these key persons have enough time allocated to the project. Further, the documentation could be reviewed for quality assurance, and the approval of the documentation could be added as a deliverable to each working package.

7.4.12 Question on adequate information to structure the work packages and get a clear understanding of tasks to be done

One interviewee points out that the project plan template is very well usable as a guideline and aids in structuring an implementation project. The interviewees further note that each organisation might cluster deliverables and work packages differently. One interviewee points out that while the dependencies of work packages are missing, the project plan is otherwise viable. One interviewee wants to add the needed persons per working package.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

7.4.13 Question on ensuring cyber-resilience after implementation

The interviewees answered this question with answers ranging from a short 'yes, definitely' to more vague answers, such as a high dependence on the current cybersecurity stance within the organisation. One interviewee added that the resulting cyber-resilience depends on the best-practise implementation of each working package. One interviewee pointed out that the project plan provides some cyber-resilience assurance. However, there might be a difference between the DORA requirements and cyber-resilience per se.

7.4.14 Question on DORA compliance after implementation

The interviewees all respond that the best-practise implementation of all work packages will comprehensively cover the DORA related requirements as they are currently known. One interviewee who was also provisioned with a snapshot of the chapter 6 found the verification very useful to demonstrate compliance and to detail work packages.

7.4.15 Question on additional feedback

When asked about additional feedback, one interviewee noted that project goals and non-goals should be added to the project plan template. Further, one interviewee pointed out that some organisations will be overwhelmed with the requirements since the interviewee rates the awareness of DORA related requirements deficient. This low awareness of requirements is especially the case in third-party risk management. This interviewee further states that the DORA mandated implementation of service management processes will overwhelm organisations because of a currently low rate of correct implementation of those processes in the industry. One interviewee added that the table on the first page of the project overview should be extended by the fields 'steering board members', 'accountable manager', and the signed management commitment for crucial resources and significant milestones.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

CHAPTER 8

Results and Discussion

The following chapter summarises, contextualises, and discusses the findings from this master's thesis.

8.1 Design Verification against Requirements

This section discusses the analytical verification against the requirements of the project plan template as laid out in chapter 6

8.1.1 Legal verification

Within the legal verification, working packages are mapped to corresponding Articles from the DORA and its surrounding RTS and ITS. While this analytical method can not guarantee that all paragraphs, subparagraphs, points, indents and sentences of each Article are covered within this project plan template, it does point out that no full Articles were left out. It further shows that using this template will be a first step towards full compliance. As pointed out by one expert in the expert interviews, realising an affectedness by a norm and starting to implement a compliance project against the requirements of this norm dramatically reduces any penalties that might arise. Therefore, covering all Articles in an initial project plan and implementing the project accordingly significantly reduces any impending charges for supervisory authorities. As pointed out during the OeNB interview, those penalties can vary substantially from an evil eye to the revocation of the banking license. Hence, using this project plan template and implementing a project resulting from this plan reduces the legal risks of noncompliance and consecutive penalties in the context of the Digital Operational Resilience Act.

Furthermore, the mapping from Articles to working packages in the project plan template can guide the implementation of working packages to plan the concrete obligations within each work package. When approaching the upfront planning of a working package,

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

searching for the package code within the described mapping section showcases which concrete obligations result for the working package and thereby reduces the time to infer all requirements for the deliverables of each working package

On the contrary, the legal verification showcased that many Articles were covered by several working packages, as in table 6.1. 12 of 18 relevant Articles in the DORA and 18 of 39 relevant Articles in the analysed RTS are covered by more than one working package. This multi-coverage entails additional research time when implementing the project plan, as the individual requirements must still be sorted into more than one working package.

In conclusion, the coverage of legal requirements resulting from the DORA and its surrounding RTS is sufficient to reduce risks resulting from supervisory penalties. Thereby, the requirement to reduce risks resulting from supervisory penalties is fulfilled.

8.1.2 Technical verification

The technical verification section in chapter 6 maps the controls of the ISO27001 to the working packages of the herein presented working plan template. The ISO27001 is the industry standard regarding information security management systems and related controls as presented in the Annex and within the ISO27002 norm. The mapping of working packages showed seven controls from the Annex not covered by the working plan template, and 100% of the controls from the ISO270001 and 92% of the controls in the Annex were covered by the project plan template. In comparison to the legal verification, the more significant fractions of 9 out of 21 chapters and 61 out of 93 controls were covered by a single working package. This lower coverage per item compared to the higher coverage in the legal verification is possibly an indicator of the higher granularity and more straightforward structure of the industry norm and the working plan template compared to the more clustered legal norm.

The mapping of chapters and controls from the industry standard to the working packages of the project plan template of this thesis showcases two things: The first conclusion is that there is a high similarity between both documents. The second conclusion is that the project plan template covers most information security and information security management system topics. This technical mapping aids the implementation efforts as financial institutions can refer to single controls and chapters when planning and implementing individual working packages. This additional aid shortens the research cycles in each working item's planning and implementation phase in addition to the legal mapping described above.

Finally, the coverage analysis of the chapters and controls of a dominant industry standard showcases that the working plan template is close to a practitioner approach to information security, a concept highly intertwined with the concept of cyber-resilience as described in chapter 4. It further demonstrates a high level of completeness in terms of topics approached in the working plan template regarding topics of cyber-resilience.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

8.1.3 Threat Mapping

Organisations' most common threats are referenced from the ENISA Threat Landscape Report 2023 [Eni23] (pages 6-8). The mapping of working packages showed that, except for information manipulation and interference, each of the so-called "primary" threats is covered by working packages of the project plan template. As mentioned in the introduction, the threat of information manipulation and interference was not prevalent within the financial sector as mentioned in the ENISA threat landscape 2023 [Eni23] (page 14). Only working packages that directly target a threat are mapped within this analysis. More general working packages that reduce the potential damage or increase the chance of detecting and reacting to a threat are not mapped.

This mapping showcases that the project plan template reduces either the likelihood that a threat materialises or the effect that a threat has on the organisation. By introducing processes such as Incident Management within the project plan template, the implementing organisation can react in a coordinated way to the threats once they materialise. This mapping showcases that the project plan template contains relevant measures to prevent, respond to, and recover from attacks and damages resulting from those primary threats, thereby reducing the risks associated with cyber threats. The requirement to enhance the cyber-resilience of an organisation is hence concluded to be fulfilled.

8.2 Findings from the Expert Interviews

The expert interviews detail several strengths and weaknesses of the project plan template. The weaknesses of the project plan template include lacking details of a project plan, being a format that must be transformed before being put into use, a lack of detailed dependencies, a missing KPI regarding the completion of the project and a lack of fine-grained details and requirements for each working package.

The strengths of the project plan template include being easy to understand, a focus on third-party management, being in a format that is easy to understand and easy to evaluate by experts and academically, being in a format that can be used as documentation, suggesting a set of valuable KPI, providing a clear overview of a possible project, providing a guideline and starting point for cyber-resilience projects, including highly relevant risks and mitigation strategies, providing enough information to structure a project, being very likely to mitigate the risk of DORA related penalties and increasing the overall cybersecurity stance of an organisation.

8.3 Discussion of Results

The expert interview evaluation reveals the different strengths and weaknesses of the project plan template. It attests that the project plan template is highly valuable in implementing cyber-resilience and DORA compliance projects. The verification part

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

reveals how well the project plan template fulfils its business requirements. While both sections show a general achievement of the requirements in chapter 5, some adjustments to the project plan template are still open for further adaptation and future research.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

CHAPTER 9

Conclusion

This chapter shortly highlights the insights of this thesis, its contributions to the field and the possibilities of future research.

9.1 Summary of the Study

This master thesis provides an overview of the information security domain regarding industry standards and legal norms. It further introduces a mapping of the influence of information security in organisations. This mapping is derived from a meta-synthesis of the literature and showcases the applicability of industry standards and legal norms within organisational structures, processes and technical systems. In addition, the different facets of resilience across scientific disciplines are discussed. In particular, the DORA, its' motivation and auditing are analysed and enriched with an interview of Austria's lead auditor at the Austrian National Bank (OeNB). Further, the master thesis details requirements for a generic artefact to guide financial institutions' cyber-resilience efforts. This generic artefact is then designed and attached to the master thesis. The author designs this generic artefact as a project plan template, including a project frame and working packages. The resulting project plan template is evaluated in an in-depth analysis against legal requirements, an industry standard for information security and common threats. An additional qualitative evaluation is performed using interviews with three practitioners considered to be experts in the fields of ICT, compliance and project management. Finally, the analytical and qualitative evaluation findings are summarised and discussed.

9.2 Contributions to the Field

This study provides a meta-narrative about the different topics and areas of application of cyber-resilience. This meta-narrative summarised as figure 3.3 can aid practitioners

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

to organise protective TOM. It further provides a structure to approach discussions, implementations and reviews in cyber-resilience. For the first time, to the author's best knowledge, the requirements laid out in DORA are put into a generic artefact, which is evaluated through the application of research methods from an academic point of view. According to the evaluation, this generic artefact adds a valuable starting point for financial entities to take a structured approach to developing their cyber-resilience.

9.3 Limitations

The thesis has the following limitations.

2nd batch of RTS and ITS: At the time of this thesis completion, new level two texts of the DORA, including the second batch of RTS and ITS, are just released and did not make it into this thesis. This second batch, however, is a very detail-oriented addition and is not likely to change the herein-presented project plan template. However, it was not included in the literature analysis of this thesis.

Sample size: The project plan template was evaluated by three experts in the field. Adding the opinion of more experts might sharpen the overall impression of the project plan template, highlight more or other strengths and weaknesses and lead to changes in the artefact that increase its value to practitioners. Adding more or different domain experts could further solidify the study.

Retrospective Additions: Within the evaluation of the project plan template, weaknesses and room for improvement are discovered. Implementing additions and corrections based on the identified weaknesses and room for improvement could likely improve the value to practitioners.

Scope Limitation: The project plan covers most obligations that result from the DORA for financial institutes. However, it does not apply to all financial institutes, as it focuses on smaller institutions which are not considered significant institutions and hence do not have the additional obligations of TLPT. This master thesis also excludes the additional obligations that central counterparties, trading venues, trade repositories or central security depositories must oblige to. It further excludes small enterprises that fall under Article 16 subparagraph 1, namely "small and non-interconnected investment firms, payment institutions exempted under Directive (EU) 2015/2366; institutions exempted under Directive 2013/36/EU in respect of which Member States have decided not to apply the option referred to in Article 2(4) of this Regulation; electronic money institutions exempted under Directive 2009/110/EC; and small institutions for occupational retirement provision" - DORA Article 16 subparagraph 1. Those smaller enterprises have fewer obligations and a so-called "Simplified ICT risk management framework".

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

9.4 Future Research Directions

The following research directions and topics for further research are open from this master thesis. This master thesis covers the working package structure and a project plan frame.

Improve the generic artefact : The created generic artefact has some weaknesses as laid out in the verification (chapter 6), in the evaluation interviews (chapter 7) and summarised in the discussion (chapter 8). Further research could aim to resolve those weaknesses and create a new project plan template with edited and additional content or in a different format.

Develop Work Packages: This thesis showcases the structure of a project plan for organisational cyber-resilience. It does not provide details of the contents of each work package - a weakness pointed out in the evaluation section. Further details containing the exact contents of each output item per work package are grounds for further research. One such research, a focus point of DORA, is the development of the ICT third-party risk management. It entails the strategy, processes, register of information, the contents of contracts, an audit of third parties, etc. Each of those topics could manifest its research as they connect with other norms within the EU member states and internationally with entirely different legal frameworks.

Extend the scope: As mentioned in the limitations section, this master thesis excludes some financial institutions from its scope. An extension to other financial institutions, an analysis of TLPT requirements or an analysis of the “simplified risk management framework” are future research directions.

EU Cyber Resilience Act: This not-yet-released norm is announced for 2024 and will result in cybersecurity requirements for digital product producers. The methodology of this thesis could be applied to this upcoming law.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

APPENDIX A

Expert Interview Guideline

A.1 Purpose

The purpose of the interview is explained to the participants as follows: The interview evaluates a template for organisations to guide them in the step-wise implementation of their cyber-resilience efforts. Therefore, the interviewee is expected to critically examine the provided document and evaluate it according to their professional opinion.

A.2 Confidentiality

The audio of the interview will be recorded through either a mobile phone microphone or, in the case of remote interviews, through the recording of the session. The recordings are only used for transcription. The interviewee can withdraw or amend any answers given throughout the interview within two weeks after receiving the written transcription. The interviewee's name and association with any organisation can be excluded from the publication upon request.

A.3 Format

Before the interview, the participants will receive the guiding template, evaluated by e-mail or, in the case of in-person interviews, on paper. The format of the interview is the standardized open-ended interview. Within this format, through either a remote conference or an in-person interview, the interviewee is asked a standardised set of questions upon which the interviewee can answer freely. The planned duration of each interview is 30 minutes. The interviewee can send further feedback regarding the session and the artefact via mail within two weeks of the interview. The interviewee can ask questions before the interview begins.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

A.4 Questions in English

1. Could you briefly overview your professional background and experience in ICT-related project management?
2. From your perspective, what are the key elements of an effective project plan?
3. From your perspective, which section or aspect of the provided document do you find particularly valuable and why?
4. Is the format and the content of the received document easy to understand?
5. Is the type of document chosen sensibly?
6. Is there another format that would improve the usability of the contents?
7. Are the implementation steps and objectives clearly defined?
8. Are the presented KPIs easy to understand, useful and easy to measure?
9. Does the document provide a clear overview and useful guide to implementing cyber-resilience projects for organisations?
10. Do the identified project risks fit with your experienced project failures or risks in the past?
11. Are the provided risk mitigation strategies correct and useful?
12. Do the contents of the project plan template provide adequate information to structure the work packages and clearly understand the tasks to be done?
13. To what extent do you agree with the statement: “Implementing all work packages will ensure a consistently high level of cyber-resilience within an organisation” and what factors influence your decision?
14. To what extent do you think implementing all work packages will ensure DORA compliance?
15. What else would you like to add as feedback to this project plan template?

A.5 Questions in German

1. Könnten Sie einen kurzen Überblick über Ihren beruflichen Hintergrund und Ihre Erfahrungen im Bereich des Managements von IKT-Projekten geben?
2. Was sind aus Ihrer Sicht die Kernelemente für einen effektiven Projektplan?

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

3. Welchen Abschnitt oder Aspekt des bereitgestellten Dokuments halten Sie aus Ihrer Sicht für besonders wertvoll und warum?
4. Ist das Format und der Inhalt des erhaltenen Dokuments leicht zu verstehen?
5. Ist die Form des Dokuments zweckmäßig gewählt?
6. Gibt es ein anderes Format, das die Nutzbarkeit des Inhalts verbessern würde?
7. Sind die Arbeitspakete und -ziele klar definiert?
8. Sind die aufgeführten KPIs einfach zu verstehen, zweckmäßig und einfach zu messen?
9. Bietet das Dokument einen klaren Gesamtüberblick und einen nützlichen Handlungsleitfaden zur Umsetzung von Cyber-Resilienz-Projekten für Organisationen?
10. Stimmen die identifizierten Projektrisiken mit den von Ihnen in der Vergangenheit erlebten Projektfehlern oder Projektrisiken überein?
11. Sind die angegebenen Strategien zur Risikominimierung korrekt und nützlich?
12. Bietet der Inhalt der Projektplanvorlage ausreichende Informationen, um die Arbeitspakete zu strukturieren und ein klares Verständnis der zu erledigenden Aufgaben zu erhalten?
13. Inwieweit stimmen Sie der Aussage zu: “Die Umsetzung aller Arbeitspakete wird ein konsistent hohes Niveau der Cyber-Resilienz innerhalb einer Organisation schaffen” und welche Faktoren beeinflussen Ihre Entscheidung?
14. Inwieweit haben Sie den Eindruck, dass die Umsetzung aller Arbeitspakete die Erfüllung der Anforderungen nach DORA gewährleisten wird?
15. Was würden Sie noch gerne als Feedback zu dieser Projektplanvorlage hinzufügen?

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

APPENDIX B

Project Plan Template

B.0.1 Executive Summary

The herein documented project touches the organisational management (B.1), the IT controls (B.2) and the technical implementation of ICT (B.3) to strengthen and establish the cyber-resilience of an organisation on all levels. Furthermore, completing this project builds towards compliance with DORA and reduces the risk of legal penalties due to violations of the DORA. The work packages of this template are documented in enough depth to understand the organisational needs of each work package; they do not contain the specific requirements of each output item. Within each work package, the organisation must research and determine the exact contents of the listed outputs by studying the related passages of the DORA and the corresponding RTS and ITS.

B.0.2 Project Frame

The following project parameters should be collected and documented for each project context.

Key Decision Maker:
Budgetary Approval Body:
Man-Days available:
Monetary Funds available:
Start Date:
Deadline:
Key Personal and their availability for the project:
Recurring meetings:

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

B.0.3 KPI

The following KPIs are a proposed set of quantitative indicators of the project success of which a subset should be carefully selected, calculated and regularly reported to management:

- On-Time Completion Percentage of Work Packages
- Total Planned Time vs Current Time Spent
- Number of Adjustments
- Number of Errors
- Team Members leaving vs. joining the Project after Initiation
- Burn Down Rate of Work Packages

B.0.4 Project Risks & Mitigation Strategies

The following are identified key project risks that could endanger the successful implementation of the project.

Scarcity of Project Resources The scarcity of personnel is the most significant risk identified to the success of this project. Members of the project team include personnel in operational roles essential to other functions of an organisation, such as the CISO, the head of the IT department, members of the legal department and the outsourcing department. Those roles are highly involved in the day-to-day business, which might delay and prevent them from fulfilling their responsibilities in this project.

To mitigate this risk, a clear commitment from management and the involved personnel to reduce their day-to-day workload must be obtained from the beginning of the project.

Gap between Documentation and Implementation If the project is carried out solely to achieve compliance with legal obligations, the documentation and implementation are at high risk of drifting apart. Whilst documentation of many aspects of this project showcases an internal process that considers ICT risks, it fails to achieve compliance, let alone digital operational cyber-resilience.

It is essential to bring enough internal resources onto the project to mitigate this risk.

Resistance to Change Financial institutions often have a long history and traditions on how the internal processes, communication, hierarchies and responsibilities work. Some aspects of this project necessitate changing how financial institutions operate. Changing long-established organisational structures is difficult as it faces resistance from employees and management.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

To implement the necessary adaptions and therefore mitigate this project risk, it is essential that the project becomes a high priority within the organisation and that the project manager in charge develops strategies that fit into the individual context of the organisation to overcome this resistance.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Work Package Enumeration

The following sections contain the work packages, the necessary inputs upon which the work package is built, and a brief description of the objectives per work package.

The work packages in this project plan template are structured by topics resembling the three-tier distinction and overall categorisation in figure 3.3.

For each work package, the following information should be defined in the individual context of each implementation project. The field “Release by:” refers to the person who decides when to start with the work package, while the field “Acceptance by:” refers to the person who determines a work package has been done.

Start Date:
Deadline:
Task Owner:
Release by:
Acceptance by:

B.1 Organisational Governance

B.1.1 WP: ICT & Information Security Strategy

Description: The ICT & Information Security defines the approach towards ICT that an organisation takes. It defines the general goals that the ICT systems are directed towards.

Necessary inputs:

- Business strategy

Objective:

- Approved ICT Strategy

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

- Approved Information Security Strategy
- ICT Reference Architecture

B.1.2 WP: ICT Risk Management Framework

Description: The ICT Risk Management Framework describes how an entity deals with the risks of using ICTs such as attacks, data misuse or errors for supported business functions.

Necessary inputs:

- Business Strategy
- ICT & Information Security Strategy
- Business Risk Strategy & Process

Objective:

- Approved ICT Risk Management Framework
- Approved ICT Risk Strategy
- Approved ICT Risk Management Process
- Defined Risk Manager

B.1.3 WP: ICT Risk Management Implementation

Description: The above-defined Risk Management Framework must be applied to assess and manage the ICT-related risk.

Necessary inputs:

- Register of all Assets
- ICT Risk Strategy
- ICT Risk Process

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Objective:

- ICT Asset Classification
- ICT Risk Analysis
- ICT Risk Treatment Plan
- Residual ICT Risk Management

B.1.4 WP: ICT & Information Security Resources

Description: The resource definition creates a clear overview of the available resources an organisation dedicates to ICT and Information Security.

Necessary inputs: The following input might be considered to determine the budget. However, the governing body of an organisation can determine the resources independent of the formalised strategies.

- Business Strategy
- ICT & Information Security Strategy

Objective:

- Detailed enumeration of resources regarding available personnel and financial budget

B.1.5 WP: ICT Organisation: 3-Lines of Defence Model

Description: The three-lines-of-defence model ensures a separation of duties between ownership, control, and assurance within financial entities.

Necessary inputs:

- ICT & Information Security Strategy

Objective:

- Approved description of the internal structure of the 3 Lines of Defence regarding ICT-related processes and corresponding departments/personnel

B.1.6 WP: Internal Control

Description: The third line of defence, according to the 3LoD model, also called the Internal Audit, reviews must review plans and processes regarding the ICT risk management framework.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Necessary inputs:

- Asset Risk Classification
- ICT Risk Scenarios
- ICT Emergency Plans
- Incident Documentations

Objective:

- Asset Risk Classification & Documentation Review
- Risk Scenario Review
- Emergency Plan Review
- Incident Analysis
- Defined Follow-Up Process

B.1.7 WP: Roles & Responsibilities

Description: The definition of ICT-related roles and responsibilities ensures a clear and specific assignment for individual team members. This definition ensures further that tasks are more likely to be handled.

Necessary inputs:

- ICT & Information Security Strategy
- Three Lines of Defence Description

Objective:

- Information Security related responsibilities listed for all positions
- Defined Outsourcing Manager
- Defined ICT Risk Manager
- Defined Crisis Manager
- Defined Crisis Communication Manager

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

B.1.8 WP: Project Management

Description: Defining project management within an organisation ensures that ICT risks are assessed and evaluated throughout projects.

Necessary inputs:

- IT & Information Security Strategy
- ICT Risk Strategy
- ICT Risk Management Process

Objective:

- Approved Project Management Guideline, including obligatory Risk Assessments
- Project Reporting

B.1.9 WP: Information Security Management System

Description: The ISMS is the framework for controlling Information Security. Defining this framework ensures a systematic approach towards establishing a coherent level of information security.

Necessary inputs:

- ICT & Information Security Strategy

Objective:

- Defined Contextualised Information Security Goals: Confidentiality, Integrity, Availability, Authenticity
- Approved Information Security Guideline
- Defined Continual Improvement Process
- Defined Management Reporting Process

B.1.10 WP: Human Ressources Information Security Strategy

Description: The HR department deals with the change of personnel within organisations. Defining an Information Security Strategy for the HR department ensures that changes within the workforce are securely managed.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Objective:

- Approved HR Information Security Strategy
- Defined Processes for Onboarding, Offboarding and Changing Positions

B.1.11 WP: Key ICT & Security Personnel

Description: This work package aims to represent an organisation's hierarchy and roles concerning ICT graphically.

Objective:

- Organisational diagram containing at least key ICT-related personnel and their roles

B.1.12 WP: Security Training & Awareness Program

Description: Information Security Awareness minimises the susceptibility to social engineering attacks and creates awareness of potentially dangerous behaviour. Furthermore, personnel with active obligations towards ICT need corresponding knowledge to fulfil their tasks securely.

Necessary inputs:

- HR information security strategy
- ICT Outsourcing strategy
- Information Security Strategy

Objective:

- Approved Awareness and Training Strategy
- Specialised Training for the IT department, the governing body & internal auditors
- Information regarding Information Security Policies & reporting channels for incidents

B.1.13 WP: Third Party/Outsourcing Management

Description: ICT third party risk management is a central part of managing ICT risk. As such, management must determine a strategy to determine which parts of its business should be outsourced and how risks resulting from outsourcing are treated.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Necessary inputs:

- ICT Strategy

Objective:

- Approved ICT Outsourcing Strategy
- Approved ICT Third Party Risk Strategy, including guidelines on critical & important functions

B.1.14 WP: Third Party/Supplier Inventory

Description: Similarly, as the organisation inventories assets, the organisation must inventory relations with ICT Third Party Provider to centralise and control ICT Third Party Provider relations.

Necessary inputs:

- Contracts with corresponding Third Parties

Objective:

- Information register on ICT third-party provider

B.1.15 WP: Third Party Risk Management

Description: Within this work package, the operational aspects of risk management are covered. Financial institutions need to assess risks regarding ICT third-party providers and classify them based on the classification of the internal business function they support. Furthermore, financial institutions must have a plan on how to assure themselves of the ICT security measures of the third party.

Necessary inputs:

- Methodology to assess ICT third party risk (ICT Third Party Risk Strategy)
- ICT Outsourcing Strategy

Objective:

- Risk Assessment & Classification on ICT third-party provider
- Audit Planning on ICT third-party provider

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

B.1.16 WP: Contract Management

Description: Contracts with ICT Third Party Providers must adhere to a particular standard to ensure that the financial institution has enough legal possibilities to ensure the security of their services. Before commencing business with an ICT third-party provider, financial institutions must perform a defined due diligence process.

Necessary inputs:

- Register of information on ICT Third Party Provider

Objective:

- Assessing contracts on legal compliance regarding outsourcing of important and critical ICT functions
- Due Diligence Process on critical and important ICT third-party provider.

B.1.17 WP: Exit Strategies

Description: Exit strategies for critical and important ICT third-party providers ensure that the organisation is prepared to overcome problems with ICT third-party providers.

Necessary inputs:

- Register of Information on the Use of ICT Third-Party Providers

Objective:

- Documented & tested Exit Plans for critical & important ICT third-party provider

B.1.18 WP: Regulatory Compliance Assessment

Description: Within a regulatory compliance assessment, the organisation determines applicable legal norms it must adhere to. Furthermore, the organisation establishes a reporting framework following applicable laws. The DORA sets the requirement for reports regarding the ICT risk management framework, incident costs, major incidents, security testing, outsourcing and due diligence.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Necessary inputs:

- Review of the ICT Risk Management Framework
- Incident Analysis
- Incident Classification
- Planned and performed Security Testing
- Register of Information on ICT Third Party Providers
- Due Diligence Process established

Objective:

- Screening for ICT regulation set up
- Reporting on ICT Risk Management Framework set up
- Reporting on Incident Costs set up
- Reporting on Major Incident set up
- Reporting on Security Testing set up
- Reporting on Outsourcing set up
- Reporting on Due Diligence set up

B.1.19 WP: Data Protection Requirements

Description: Organisations must protect personal data to ensure compliance with the GDPR and minimise the risk to individuals.

Necessary inputs:

- Overview of all data

Objective:

- GDPR Compliance check
- Determination of 'high risk' data processing
- Data Protection Impact Assessments for 'high risk' data processing

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

B.2 IT Controls

B.2.1 WP: Asset Management

Description: Asset Management identifies, documents, and accompanies assets throughout their life cycle. The organisation must implement Asset Management as a basis for other processes, including IT operations, BIA, risk management, etc.

Necessary inputs:

- Information Security Strategy

Objective:

- Documented Asset Management Policy
- Register of all ICT assets
- Documented links & interdependencies between assets and business functions
- Classification of all ICT assets

B.2.2 WP: Quality/Cyber-Resilience Testing Strategy

Description: Financial institutions must systematically direct their testing efforts on cyber-resilience by defining a testing strategy for functional and security testing of their ICT systems.

Necessary inputs:

- Approved Budget for Cyber-Resilience Testing
- ICT reference architecture

Objective:

- Approved Testing Strategy, including levels and scope of tests

B.2.3 WP: IT Operations Management

Description: Operating ICT systems ensures their availability and integrity. Organisations must document the ICT operation processes for their ICT system by creating system descriptions.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Necessary inputs:

- Information Security Strategy
- Asset Register

Objective:

- ICT system descriptions, including the underlying data, the secure life cycle of ICT assets, requirements regarding update, backup & restore procedures, scheduling, protocols, segregation requirements and error handling

B.2.4 WP: Configuration Management

Description: The configuration management provides information about the rolled-out configuration of ICT assets. This information is vital for vulnerability management, error detection and consistent system behaviour.

Necessary inputs:

- Information Security Strategy
- Optional: Asset Register
- Optional: ICT reference architecture

Objective:

- Implemented Configuration Management Database

B.2.5 WP: Availability Management

Description: The organisation must ensure the availability of its ICT systems and supported business functions by identifying the demand and the capabilities of its ICT systems and adjusting the corresponding capacity.

Necessary inputs:

- ICT reference architecture
- ICT system description (Asset Management)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Objective:

- Identified capacity requirements for ICT systems
- Implemented capacity redundancy
- Implemented measures and processes to detect and prevent shortages

B.2.6 WP: Mobile Device Management

Description: This work package introduces a centralised management solution for endpoint devices that ensures that the organisation manages the administration of devices. The user must not be able to deviate from the defined organisation's security policies regarding endpoint devices.

Necessary inputs:

- ICT reference architecture
- Enumeration of endpoint devices (Asset Management)

Objective:

- Implementation of a Mobile Device Management system, managing data storage, applications, updates and remote wiping.

B.2.7 WP: Vulnerability Management

Description: Vulnerability management ensures that vulnerabilities in ICT systems are discovered and managed. Therefore, the organisation must establish a formal vulnerability management process and internal vulnerability reporting.

Necessary inputs:

- Information Security Strategy

Objective:

- Documented Vulnerability Management Process
- Internal vulnerability reporting set up

B.2.8 WP: Threat Intelligence

Description: Financial institutions must set up internal Threat Intelligence by identifying and using sources for threat information.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Necessary inputs:

- Information Security Strategy

Objective:

- Identified channels of threat information

B.2.9 WP: Incident Management

Description: Financial institutions must define their Incident Management Process to identify, treat and prevent ICT-related incidents. Furthermore, the scheme for classification aids in differentiating the reaction to ICT related incidents according to set criteria.

Necessary inputs:

- Information Security Strategy

Objective:

- Documented Process to identify, treat and prevent ICT-related incidents
- Documented Classification Scheme for incident classification

B.2.10 WP: Business Continuity Management

Description: The Business Continuity Management ensures that business functions of the organisation continue to operate under duress. Defining a BCM guideline ensures a systematic approach to BCM. Financial entities must further specify how their ICT assets are included in the BCM.

Necessary inputs:

- Information Security Strategy
- Register of Assets and their supported business functions.
- ICT-related key personnel

Objective:

- Approved Business Continuity Guideline concerning ICT
- Business Impact Analysis

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

B.2.11 WP: Backup Management

Description: The backup management ensures that data can be restored in case of data loss on running ICT systems. The organisation must implement a process to select and back up data.

Necessary inputs:

- Information Security Strategy
- ICT reference architecture
- Register of information assets and their classification

Objective:

- Process Description of backups including scope, frequency and recovery process of data
- Defined Return Time Objective (RTO)s and Return Point Objective (RPO)s of data

B.2.12 WP: Crisis Communication

Description: During a crisis, the need for communication arises within the organisation. To ensure a structured approach, the organisation must define communication structures during a crisis beforehand.

Necessary inputs:

- Information Security Strategy
- Business Impact Analysis
- Risk Scenarios from the BIA

Objective:

- Incident Communication Plans with customers, employees, partners and authorities
- Defined crisis communication manager

B.2.13 WP: Restore & Recovery Planing

Description: The restore and recovery planning goes beyond data and defines how ICT systems can be restored and recovered as a whole after ITSCM measures bridged any outages of ICT systems.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Necessary inputs:

- Information Security Strategy
- Backup Process Description
- BIA

Objective:

- Defined plans to restore & recover ICT systems
- Successful restore & recover test

B.2.14 WP: Emergency Exercises & Tests

Description: Organisations prepare themselves for emergencies. To understand how well those preparations work, they must test them. Therefore, the organisation must define reasonable emergency scenarios.

Necessary inputs:

- Information Security Strategy
- BIA

Objective:

- Defining Emergency Test Scenarios
- Define and implement schedule and scope of Business Continuity Plan Tests
- Define and implement schedule and scope of Response & Recovery Plan Tests
- Define and implement the schedule and scope of Crisis Communication Plan Tests
- Define and implement the process to deal with and report test results

B.2.15 WP: Cryptography

Description: The organisation must define how their ICT systems implement cryptographic controls (encryption, signatures, etc.) to meet the organisation's information security goals.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Necessary inputs:

- Information Security Strategy
- Information Classification Scheme

Objective:

- Defined rules for the encryption of data in use, at rest and in transit
- Defined rules for the encryption of network traffic
- Defined rules for the exchange of data with third parties
- Defining acceptable algorithms

B.2.16 WP: Key Management

Description: The organisation must define how they manage the life cycle of cryptographic keys, key material and certificates.

Necessary inputs:

- Information Security Strategy
- Guideline on the use of cryptography

Objective:

- Cryptographic key management policy covering the full life cycle of key material
- Register of all certificates and related hardware

B.2.17 WP: Authentication

Description: The organisation must define and implement appropriate ways of authenticating their users on their ICT systems and define under which circumstances a method of authentication is sufficient.

Necessary inputs:

- Information Security Strategy

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Objective:

- Defining appropriate authentication methods according to classification and risk profiles

B.2.18 WP: Data Erasure & Disposal

Description: To ensure data remnants on ICT systems are securely deleted and to protect the confidentiality of information, the organisation must implement processes to securely get rid of unwanted data in ICT systems and on data storage devices.

Necessary inputs:

- Information Security Strategy
- Asset Register

Objective:

- Defined process documentation regarding the collection and deletion of unnecessary data
- Defined process documentation regarding the secure decommissioning of data storage devices

B.2.19 WP: Security Configuration Baseline

Description: The organisation must define and implement a consistent technical guideline of default/minimal security standards to be applied to all ICT systems to ensure consistency in security settings.

Necessary inputs:

- Information Security Strategy
- ICT reference architecture

Objective:

- Defined secure configuration baseline for endpoints, servers, databases & network components
- Defined measures to ensure the application of the baseline

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

B.2.20 WP: Change Management

Description: Implementing change management ensures that the risk of alterations to ICT systems are identified, evaluated and minimised.

Necessary inputs:

- Information Security Strategy

Objective:

- Defined Change Process, including security checks & risk analysis

B.2.21 WP: Patch & Release Management

Description: Organisations must apply patches and updates as part of the maintenance of ICT systems. To ensure that risks during patches and updates are minimised, organisations must define and implement processes that identify, evaluate & treat the corresponding risk.

Necessary inputs:

- Information Security Strategy
- Optional: Change Management Process

Objective:

- Defined Patch & Release Process, including an evaluation, an emergency procedure & testing

B.2.22 WP: Software Development Lifecycle

Description: Depending on whether the financial entities develop their own ICT services or outsource their development, they must implement measures to protect any source code, compiled or raw, from tampering.

Necessary inputs:

- Information Security Strategy

Objective:

- Implemented proportionate integrity protections of source code

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

B.2.23 WP: Requirements Management

Description: To establish a high level of security and functionality and to better understand the ICT systems the organisation uses, the organisation must develop a guideline on the acquisition, development and maintenance of ICT systems. Within these guidelines, the development of requirements of ICT systems must be established.

Necessary inputs:

- Optional: ICT Risk Management Strategy
- Optional: Project Management Guideline/Process

Objective:

- Guideline on the acquisition, development and maintenance of ICT systems, including functional & nonfunctional requirements and approval of security requirements

B.2.24 WP: Identity Management

Description: Users of ICT systems undergo a life cycle that must be defined and managed by the organisation to ensure all user management systems manage all users from creation to deactivation.

Necessary inputs:

- Information Security Strategy

Objective:

- Defined Identity Lifecycle Management

B.2.25 WP: Access Rights Management

Description: Access rights management regulates the objects and actions that identities can perform. The organisation must manage the access right life cycle to ensure that users have only the correct access rights.

Necessary inputs:

- Information Security Strategy

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Objective:

- Guideline minimizing access rights, including general access rights principles
- Removal/minimization of shared accounts
- Defined Access Rights Process (Grant, Review, Removal)

B.3 Technical Implementation

B.3.1 WP: Physical Security

Description: The organisation must establish physical security as the basis for the security of its infrastructure. Their ICT systems and information processing facilities must be physically secured through a policy and TOM.

Necessary inputs:

- Information Security Strategy
- Optional: ICT reference architecture
- Optional: Facility Plans

Objective:

- Defined physical & environmental security policy
- Implemented physical security measures

B.3.2 WP: Network Security

Description: Network security ensures an organisation's communication confidentiality, integrity, and availability. Networks must be protected through several TOM.

Necessary inputs:

- ICT reference architecture

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Objective:

- Mapping and visual representation of networks
- Network Security Policy
- Network Access Control (NAC)
- State-of-the-Art network encryption
- Review of the network architecture
- Regular review of connections filters and firewall rules
- Implemented Session timeouts
- SLA on network services

B.3.3 WP: Segmentation & Isolation

Description: Network segmentation is one of the most effective measures to limit lateral movements of attacks. Organisations must implement a set of segmentation and isolation measures to prevent the escalation of an attack.

Necessary inputs:

- Mapping and visual representation of networks
- Security Baseline

Objective:

- Network segmented according to risk profile and classification of underlying ICT assets
- Dedicated administration network
- Automated isolation mechanisms for ICT assets

B.3.4 WP: Data Loss Prevention

Description: Data Loss and Leakage can result in the compromise of confidential information. When protecting their intellectual property and the confidentiality of information, the organisation must protect itself from malicious and negligent insiders to detect the unauthorised loss or leakage of data.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Necessary inputs:

- Enumeration of endpoints (Asset Management)

Objective:

- Implemented DLP measures or a full fledged DLP system

B.3.5 WP: Endpoint Protection

Description: To protect endpoints against malicious code, an organisation must implement security measures to detect and isolate malicious activities on endpoint devices.

Necessary inputs:

- Mobile Device Management

Objective:

- Managed Antivirus malware protection on all endpoints.

B.3.6 WP: Logging

Description: Logs are an important part of detecting and analysing ICT related security incidents. Creating, collecting and storing logs is an essential part of monitoring ICT system. Therefore, the organisation must create and implement a logging concept.

Necessary inputs:

- Register of ICT assets
- System descriptions

Objective:

- Identified events and defined level of detail to be logged
- Defined retention periods
- Measures to secure and handle the logs
- Detection of failures of logging systems

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

B.3.7 WP: SIEM/SOC

Description: The organisation must implement measures to detect anomalies in their systems. A centralised log collection and analysis through a Security Information and Event Management (SIEM) or a SOC ensures detection and reaction. The organisation must protect these systems.

Necessary inputs:

- Logging concept

Objective:

- Automated continual monitoring for performance bottlenecks and incident-related anomalies
- Defined reactions and alarms resulting from identified events, including documentation of resulting activities

B.3.8 WP: Entrance Controls, Intrusion Protection

Description: Physical security of the organisation's facilities ensures that only authorized personnel and devices enter the facilities and physical networks. Therefore, the organisation needs to control who and what enters its facilities and prevent unauthorized entries.

Necessary inputs:

- Facility plans

Objective:

- Policy on the physical security of premises and data centres
- Definition of a perimeter concept with different sensitivity levels and appropriate protection measures
- Protection measures towards unattended ICT assets

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

APPENDIX C

Transcripts of Expert Interviews

C.1 Interview 1

The following conversation was held between Jonathan Denzel and Markus Hefler on 18. December 2023 via remote video call in German.

C.1.1 Transcript

Jonathan Denzel: Hallo, Markus. Danke dass du dich bereit erklärt hast heute mitzumachen.

Markus Hefler: Hallo, gerne.

Jonathan Denzel: Ich glaube, der Sinn und Zweck hinter dem Interview ist klar: Ich möchte mein Projektplan Template evaluieren. Für meine Masterarbeit. Ich werde entsprechend dieses Gespräch - wenn es für dich in Ordnung ist - aufnehmen, transkribieren und dir dann nochmal zur Einsicht schicken und ansonsten dann mit veröffentlichen - hinten im Anhang, das Transkript davon. Das Format sollte auch klar sein. Wir werden etwa eine halbe Stunde brauchen. Ich habe hier einmal die Fragen auf Englisch und auf Deutsch. Ich denke, wir gehen sie dann auf Deutsch durch, auch wenn das Dokument auf Englisch ist.

Markus Hefler: Wie du möchtest, aber wir können das gerne auf Deutsch machen. Passt schon.

Jonathan Denzel: Ja, passt. Magst du nochmal einen kurzen Überblick über deinen beruflichen Hintergrund geben und deine Erfahrung im Bereich vom ICT Projektmanagement?

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Markus Hefler: Ja. Also beruflicher Hintergrund und die Erfahrung im Bereich IKT - als Überbegriff jetzt - ist im Raiffeisensektor mittlerweile über 14 Jahre groß und davor habe ich schon fünf Jahre wirklich operativ als Systemadministrator bei einem metallverarbeitenden Unternehmen gearbeitet und davor -. Mein erster Job war der, eines damals noch sogenannten EDV Trainers. Das heißt, ich habe dort die angehenden Systembetreuer geschult in der Administration von Windows und Linux. Beispielsweise UNIX-Systeme, Netzwerk, Security von Netzwerksicherheit vor allem; Firewall Regeln schreiben, Desktopapplikationen einrichten usw. Also einiges an beruflicher Erfahrung mittlerweile. Im Raiffeisen Sektor im Speziellen habe ich das Thema Informationssicherheit aufgebaut im steirischen Raiffeisen Rechenzentrum. Das es jetzt in dieser Form nicht mehr gibt. Sondern das ist auch in Österreich mittlerweile angekommen, 'Economy of Scale' also in eine größere Einheit fusioniert und habe dort eben die Informationssicherheit auf der ISO-27001 Norm aufgebaut und auch zertifizieren lassen. Und die Zertifizierung solange ich dort tätig war auch weitergeführt, auch das Thema IT-Service Management hab ich mit aufgebaut - das liegt mir auch nach wie vor sehr am Herzen wobei ich damit beruflich mittlerweile weniger damit zu tun hab. Auch die wirklich Rechenzentrum-spezifischen Normen TIA-942 und der Nachfolger, das europäische Pendant eigentlich EN-50600, vorbereitet und auch maintained. Das letzte Thema was war, war dann die Zertifizierung auf den Normen 27018 und 27017 im Sinne von Cloud Provider. Das war das Normenumfeld. Und jetzt, seit einigen Jahren, in der Raiffeisen Landesbank Steiermark habe ich auch zusätzlich das Thema Datenschutz mit übernommen und auch den juristischen Datenschutz als Datenschutzbeauftragter, wo mich eben zwei Datenschutz-Juristinnen unterstützen in der Umsetzung. Die Kunden sind sämtliche steirischen Raiffeisenbanken. Zusammen aktuell 44 plus eben das Raiffeisen Competence Center für das Thema Informationssicherheit, Datenschutz und mittlerweile auch der Governance - das ist das dritte Standbein. Wo ich ein Data Access Framework mitaufgebaut habe. Wo es darum geht, die Datennutzung mit möglichst geringen Aufwand zu einem Maximum zu erheben. Das heißt, immer größere Datenmengen - wollen wir schauen, mit einem möglichst kleinen Aufwand zu verwalten, das alles detailliert darzustellen, andererseits auch aus den Compliance-Gesichtspunkten. Also ich rede immer von IT Compliance - nicht nur speziellen Themen, sondern generell, was jetzt IT oder IKT Compliance betrifft- zusammenfasst und dann pro Projekt für meine eigene Checkliste zum Beispiel implementiert, dass sämtliche Auslagerungen und IT-Applikationen auch standardisiert überprüft werden und dass immer derselbe Standard an eine Auslagerung angelegt wird. Und abschließend noch das Thema internes Kontrollsystem. Das ist auch in meiner Verantwortung aktuell auch - war, kann man fast schon sagen - für die Raiffeisen Landesbank Steiermark.

Jonathan Denzel: Sehr gut. Vielen Dank für den Einblick. Was sind aus deiner Sicht die Kernelemente für einen effektiven Projektplan im Bereich IKT?

Markus Hefler: Effektive Projektplanung IKT? Wichtig ist die Abstimmung. Bevor man mit dem Projekt startet - muss man eigentlich sagen, ist das jetzt eigentlich die Vorstufe zum eigentlichen Projektplan - die Abstimmung mit den relevanten Stakeholder

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

im Vorfeld. Und als erster Punkt oder wichtiger Punkt ist die Abstimmung mit den jeweiligen Stakeholdern. Was haben Sie eigentlich für Erwartungen? Welche Ziele? Zieldefinition ist ein ganz wesentlicher Punkt, der leider in der Praxis oft, entweder vergessen oder stiefmütterlich behandelt wird. Weil dadurch passiert es eben oft, dass IKT Projekte an den Erwartungen der Stakeholder vorbeigehen. Im Sinne von Ziele definiert werden, die zwar als Projekt sinnvoll sind, aber gar nicht gewünscht sind von den Stakeholdern. Das sind so meine Erfahrungen in diesen IKT Projekten, auch bei den Zertifizierungsprojekten, zum Teil, aber ganz stark war zum Beispiel das Thema MS365 Einführung in der Raiffeisenbank Gruppe Steiermark. Das habe ich zusammen mit einem Kollegen geleitet, wo man von Lotus Nodes auf ein MS365 Produktportfolio migriert hat. Und dort hat es durchaus Stimmen gegeben, wo man gesagt hat okay, hätte man vorher mit den Stakeholdern intensiver gesprochen, dann wäre das Projekt vielleicht auch anders gelaufen.

Jonathan Denzel: Okay. Ja, vielen Dank, denn ab jetzt sind die Fragen eher spezifisch zu meinem Projektplan, den ich geschrieben habe. Hattest du schon die Möglichkeit drüber zu schauen?

Markus Hefler: Leider noch nicht.

Jonathan Denzel: Dann gehen wir drüber. Wir haben einmal die Executive Summary, wo ich sage, es gibt irgendwie drei Ebenen von diesem Projektplan. Das erste ist diese internen Governancethemen, wo auch um die Organisationsstruktur sich drehen. Der zweite Teil sind die IT Control Prozesse und der dritte Teil sind die technischen Implementationen davon. Und das Ziel von diesem Projektplan ist einmal organisatorische Cyber Resilienz aufzubauen und gleichzeitig mit der DORA compliant zu werden und damit dann auch die rechtlichen Strafen, die da damit einhergehen, falls man nicht compliant ist, zu minimieren. Das ist die Executive Summary von dem Ganzen. Es orientiert sich natürlich an der DORA und den darunterliegenden verbindlichen technischen Standards. Das Zweite, was glaube ich wichtig ist, bei so einem IKT Projekt ist, ist einmal den Projektrahmen zu bestimmen. Das sind im Prinzip die Stakeholder. Hier erst mal wer sind die Key-Decision-Maker dabei? Wer gibt das Budget frei dafür? Wie viele Mann-Tage sind dafür tatsächlich verfügbar? Wie viel Geld dafür ist noch zusätzlich verfügbar? Wann geht's los? Wann soll es fertig sein? Wer ist alles mit involviert? Schlüsselpersonen? Und wie viel Verfügbarkeit haben die? Und welche wiederkehrenden Meetings gibt es alle im Rahmen von diesem Projekt?

Markus Hefler: Wenn ich noch etwas ergänzen dürfte oder einen Input geben dürfte, Projektziele würde ich aufnehmen.

Jonathan Denzel: Wie bitte? Projekt?

Markus Hefler: Projektziele und Projekt-nicht-Ziele. In dieser Liste.

Jonathan Denzel: Okay.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Markus Hefler: Ja, weil das wird oft vernachlässigt und hat aber wesentlichen Einfluss auf den Erfolg des Projekts.

Jonathan Denzel: Danke dafür schon mal! Dann der dritte Teil von diesem Intro ist noch die KPIs, die man mit so einem Projekt verbinden kann, damit man es entsprechend steuern kann. Das ist eine Sammlung an, unter Umständen, sinnvollen KPIs, von denen man sich welche aussuchen sollte, je nachdem wie einfach sie zu berechnen sind, ob man interne Zeitaufzeichnungen hat oder nicht. Entsprechend sind es jetzt mal sechs Vorschläge. Das erste ist On-Time-Completion-Percentage. Wie viele Arbeitspakete hat man im richtigen Zeitrahmen abgeleistet? Dann wie viel Zeit haben wir schon verbraten von dem, was wir geplant hatten ursprünglich? Die Anzahl an Veränderungen am Projektplan und an der Projektplanung? Die Anzahl an Fehlern, die dabei gemacht wurden? Die Team Member, die gegangen sind bzw. noch dazugekommen sind, nachdem man es initiiert hat? Und die Burndown-Rate von den Work-Packages? Also in welcher Zeit haben wir bisher die Arbeitspakete erledigt und was visieren wir eigentlich an? Liegt es noch innerhalb der Deadline? Das sind so die KPIs, die ich da vorschlage.

Markus Hefler: Ja, das ist okay. Wie gesagt, wie du schon richtig gesagt hast, es hängt immer davon ab, wie das Projekt an sich funktioniert. Wir sehen jetzt gerade wie die Zeit aufgezeichnet wird, wie verlässlich funktioniert das? Aber das sind allgemeine Themen.

Jonathan Denzel: Ja, voll. Und der vierte Teil von diesem Intro sind Projektrisiken und mögliche Umgehungsstrategien, die bei so einem Projekt auftreten können. Das eine ist eine Knappheit von Projektressourcen, ist glaube ich auch klar, was damit gemeint ist, nachdem die IT und die Informations-Security meistens dünn ist in vielen Unternehmen - dünn aufgestellt ist, weil sie teuer ist auch. Und da ist die Mitigationsstrategie: Man braucht vom Management erst mal ein klares Commitment zu diesem Projekt und am Ende muss auch dieser Day-to-Day Workload von denjenigen, die involviert sind, reduziert sein. Ansonsten hat so ein Projekt schon ein paar Geburtsfehler mit drin. Das als Strategie vielleicht von Anfang an mitzubedenken.

Das nächste Risiko, das ich identifiziert habe, ist, dass es einen Gap gibt zwischen Dokumentation und Implementation. Und auch da ist eigentlich die Hauptrisiko-Mitigationsstrategie, genügend Ressourcen mit reinzubringen, nicht nur die Dokumentation anzupassen, sondern auch wirklich in die einzelnen Strukturen überhaupt einen Impact bringen zu können. Weil ich glaube, wenn man nicht genügend Ressourcen zur Verfügung hat, dann hat man dieses Risiko wesentlich höher, dass man nur die Dokumentation dazu anpasst. Und das letzte Projektrisiko ist Resistenz zu Change, dass sehr viele Prozesse lang etabliert sind und sich nicht ändern wollen. Und ich glaube, da kann die einzige Strategie sein, dass man sagt, man hat eine sehr, sehr hohe Priorität, die man diesem Projekt zuordnet und sagt, gewohnte Traditionen müssen dem weichen und diese Nachricht im Prinzip schon von Anfang an bei Projektinitiationen mit reinbringt.

Du grinst?

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Markus Hefler: Ja, ja. Ich grinse nur deswegen - nicht dass das jetzt nicht richtig wäre - aber ich denke immer daran, das ist natürlich von Unternehmen zu Unternehmen unterschiedlich. Aber ein Unternehmen ist beratungsresistenter als das andere bzw. festgefahrener in seinen bestehenden Prozessen als andere, also traditionell vs. agil. Hängt natürlich auch mit dem Alter des Unternehmens zusammen. Aber in den meisten Fällen - weil du gesagt hast, die Priorisierung des Projektes muss man erhöhen als Gegenmaßnahme - hängt, wie gesagt, stark vom Unternehmen ab. Bei uns im Unternehmen würde das, zum Beispiel, wenig Erfolg bringen. Das einzige, was in unserem Unternehmen zum Erfolg führen könnte, ist, wenn das Management Commitment des Gesamtvorstands in dem Fall und die Weiterfolge des CEOs entsprechend gehoben wird. Also nur das Projekt zu priorisieren ohne das entsprechende Management Commitment hängt da, funktioniert zum Beispiel in unserem Unternehmen nicht. Das ist nur als Input jetzt gesehen.

Jonathan Denzel: Okay, danke schön.

Markus Hefler: Und als zusätzliches Risiko vielleicht, weil du möchtest nur als Input, wie gesagt, ob du das aufnimmst oder nicht ist deine Sache.

Aber ein wesentliches Risiko in diesem Fall jetzt der Unternehmen ist es, dort das fehlende Fach Know-how bereitstellen zu können, um die Anforderung, der DORA richtig interpretieren zu können und in weiterer Folge auch entsprechend umsetzen zu können. Also einerseits haben wir die dünne Personaldecke, was die Cybersecurity betrifft, aber DORA betrifft ja jetzt nicht die klassische Cybersecurity sondern betrifft ja ganz stark Resilienz. Halt das Thema BCM oder IKT Risikomanagement. Das heißt, wenn alle drei dieser Fachdisziplinen - oder vier sind es im Endeffekt in der weiteren Folge - dünn besetzt sind, dann hast du natürlich in allen vier Bereichen wenig Know-how bzw. wenn es, weil es ja gerade stark um das Thema Outsourcing geht. Wenn man Vorgaben geben muss und definieren muss für seine Outsourcing-Dienstleister, wo es jetzt auch rechtliche Implikationen hat, im Sinne von man die Standardvertragsklauseln einbauen und so weiter. Also da sind schon viele Dinge drinnen, die auch ein fachliches Know-how bedürfen, um die korrekt umzusetzen. Da sehe ich ein riesiges Risiko. Zusätzlich.

Jonathan Denzel: Okay. Ja. Danke dafür. Dann bin ich mit diesem Überblick fertig, mit diesem Projektrahmen. Und dann kommen die einzelnen Work-Packages, die ich identifiziert habe. Und die orientieren sich an dieser Dreiteilung von Organisation, IT-Prozesse und technische Implementierung. Und da habe ich für jedes einzelne Work-Package eben diese fünf Themen/fünf Keywords identifiziert. Wann geht das Work-Package los? Wann soll es fertig sein? Wer ist der Owner von diesem Work-Package? Wer sagt am Ende: Jetzt sind wir damit fertig? Und wer sagt: Damit bin ich einverstanden. Und ich glaube, diese fünf Fakten gilt es zu jedem einzelnen Arbeitspaket zu definieren. Du nickst. Sehr gut. Dann gehen wir rein. Das erste ist die IKT & Informations-Sicherheitsstrategie, dass ich ausgemacht habe, dass man damit anfängt. Was braucht man dafür? Die Businessstrategie als ausformulierten Input. Und rauskommen soll die IKT Strategie und die Informationssicherheit Strategie sowie die IKT Referenzarchitektur.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Und so zieht sich das jetzt durch die nächsten - durch diese Arbeitspakete durch - die im Folgenden kommen.

Hast du dieses Dokument bei dir offen? Ich hatte es dir per Mail geschickt.

Ich kann dich da gerne durchführen. Ansonsten könntest du dir jetzt vielleicht auch fünf Minuten Zeit nehmen, um das mal zu überfliegen. Was du von diesen Paketen hältst. Sonst rede ich mich fusselig.

Markus Hefler: Ich verstehe. Ich verstehe. Moment. Ich habe es schon aufgemacht. Ich schaue es mir kurz durch. Moment.

Wo ich gerade dabei bin: B 1.8. Work-Package: Projektmanagement. Auf der Seite elf.

Jonathan Denzel: Ja, habe ich.

Markus Hefler: Im Projektmanagement Specialized Evaluated Projekts. Ja. Ist das korrekt? Ist das alles ein Arbeitspaket? Es ist das erste generelle Projektmanagement in dem Sinne, wie Projekte abgewickelt werden. Das ist bei uns im Projektleitfaden, im strategischen Projektmanagement angesiedelt. Das heißt wir haben das - ich spreche jetzt aus unserer Erfahrung- da hat man diese Projektrahmenbedingungen - sagen wir dazu- sind in einem Projektleitfaden definiert und aber nicht das Arbeitspacket das in den einzelnen Projekten festgehalten wird, das heißt man geht von bestehenden Rahmenbedingungen aus und definiert nur die in Projekte behandelten Arbeitspakete, aber nicht das generelle Projektmanagement. Nur als Input.

Jonathan Denzel: Also der Gedanke dahinter ist, dass DORA vorschreibt, dass auch im Projektmanagement von Unternehmen genau in diesem Projektleitfaden, den ihr intern benutzt, dass da in allen möglichen Phasen Risiko Assessments gemacht werden für IKT-Risiken. Und wenn jetzt dieses Arbeitspaket drin ist, dann bezieht sich das nicht auf dieses DORA Projekt, sondern auf das Projektmanagement insgesamt im Unternehmen.

Markus Hefler: Okay, du meinst, dass das Projektmanagement, das im Unternehmen implementiert, auch die DORA Anforderungen berücksichtigt? Na dann passt das.

[Markus Hefler geht die Arbeitspakete durch]

Third Party/Outsourcing Management...

Jonathan Denzel: Ja, natürlich. Das habe ich in mehrere eingeteilt, in mehrere Arbeitspakete.

Markus Hefler: Das ist eines der größten Themen innerhalb der DORA, meiner Meinung nach.

Jonathan Denzel: Mit Sicherheit. Weil der, glaube ich, viele unerwartet treffen wird.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Markus Hefler: Ja.

Markus Hefler: Und der Umfang ist nicht zu unterschätzen. Nicht, dass es nicht schon gemacht werden würde, aber der Umfang der Umsetzung der wird einige recht kalt erwischen. Behaupte ich jetzt einmal.

Markus Hefler: Sehr gut. Genau.

[Markus Hefler geht die Arbeitspakete weiter durch]

Ja das sind die Service Management Prozesse die relevant sind.

Markus Hefler: Da rächt es sich wieder wenn man diese Service Management Prozesse noch nicht im Einsatz hat, muss man die Service Management Prozesse erst einmal richtig oder überhaupt erst mal implementieren.

Das unterschätzen auch viele Unternehmen, mit denen ich schon darüber gesprochen hab. Andere Unternehmen.

Markus Hefler: Bei B3.7 SIEM/SOC

Jonathan Denzel: Ja.

Markus Hefler: Du gehst davon aus, dass das Unternehmen ein SIEM System hat bzw. ein SOC betreibt oder beauftragt wird.

Jonathan Denzel: Nein, ich gehe davon aus, dass die Funktionen, die von der Dora gefordert werden, in diesen Bereichen innerhalb von diesem Arbeitspaket angesprochen werden.

Markus Hefler: Das ist der wesentliche Unterschied, ob man davon ausgeht, dass es vorhanden ist oder ob man sagt, die Funktionen müssen definiert werden. Wie auch immer man das dann entweder intern oder auch extern vergibt.

Jonathan Denzel: Ja, perfekt. Dann schauen wir noch mal kurz auf meine Fragen, die ich dann dazu habe noch, die wir noch nicht angesprochen hatten. Welcher Abschnitt oder Aspekt des bereitgestellten Dokuments ist aus deiner Sicht besonders wertvoll und warum?

Markus Hefler: Ja, der Aspekt des Third Party Riskmanagement bzw. Supplier-Management. IKT. Also in dem Fall ein ganz wichtiges Thema. Wie gesagt, aus meiner Sicht das zentrale Element der DORA Verordnung an sich, weil das sicher der Bereich ist, der die meisten Unternehmen am kältesten erwischt, wenn ich das so ausdrücken darf. Weil die anderen Themen wie, ich sage einmal, BCM in seiner Gesamtheit - mit den ganzen Subthemen von Kommunikation, Notfalltests, Durchführung, wie kommuniziere ich und die ganzen Exit-Strategien- die müssten schon aufgrund der schon seit Jahren

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

gültigen EBA-Guidelines umgesetzt sein und etabliert sein. Wohingegen, es gibt zwar diese EBA-Guideline mit dem Outsourcing Management, ja, aber die ist im Vergleich zu anderen noch relativ jung und sicher noch nicht so etabliert wie andere Richtlinien. Also von dem her bin ich der Meinung, dass das Thema Outsourcing in seiner Gesamtheit, also auch das Vertragsmanagement im Sinne von Standardvertragsklauseln einführen und hin und her und auch entsprechend die internen Richtlinien für die Vorgaben, wann unter welchen Voraussetzungen ich welche Dienstleistung beauftragen darf - für die Zukunft sicher einer der größten Fallstricke sein wird.

Jonathan Denzel: Okay, danke schön. Ist das Format und der Inhalt des Dokuments leicht zu verstehen?

Markus Hefler: Format finde ich sehr gut und das ist aus meiner Sicht auf jeden Fall auch verständlich.

Jonathan Denzel: Dankeschön. Die Form des Dokuments. Ich habe da am Anfang eine Weile überlegt, bringe ich es in eine Excel, mache ich es einfach als Papier. Würdest du da sagen, die ist zweckmäßig gewählt?

Markus Hefler: Für das Projektmanagement, um das abzuarbeiten oder für einen Leser, damit er einen Überblick bekommt? Was ist da der Sinn oder das Ziel von dem Dokument? Wer sind die Stakeholder? Wer sind die Empfänger? Das ist jetzt die Frage für mich.

Jonathan Denzel: Das ist eine sehr gute Frage. Nachdem es ein akademisches Projekt ist, geht es wahrscheinlich eher erst mal an Leser. In der Praxis wäre sicher noch mal ein anderes Format.

Markus Hefler: Ja. Also für die Arbeit an sich passt es. Für die praktische Anwendbarkeit wäre natürlich ein Excel oder irgendein anderes Projektmanagement Tool sicher handhabbarer.

Jonathan Denzel: Okay, perfekt. Ist die Frage 6 auch geklärt. Sind die Arbeitspakete und Ziele aus deiner Sicht klar definiert?

Markus Hefler: Ja.

Jonathan Denzel: Perfekt. Zu den aufgeführten KPIs: sind die verständlich, zweckmäßig und einfach zu messen?

Markus Hefler: Die ersten beiden ja. Letzteres, muss ich ganz ehrlich sagen, it depends. Das hängt ganz stark vom jeweiligen Unternehmen ab und von den Projektumfeldern. Ja, das ist sehr stark schwankend.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Jonathan Denzel: Würdest du sagen, das Dokument bietet einen klaren Gesamtüberblick und einen nützlichen Handlungsleitfaden zur Umsetzung von DORA Projekten?

Markus Hefler: Definitiv ja.

Jonathan Denzel: Sehr gut. Stimmen die identifizierten Projektrisiken mit den von dir in der Vergangenheit erlebten Projektfehlern oder Projektrisiken überein?

Markus Hefler: Wie gesagt, das, was ich eingangs erwähnt habe, aber sonst ja.

Jonathan Denzel: Sind die angegebenen Strategien zur Risikominimierung nützlich und richtig?

Markus Hefler: Sind auf jeden Fall nützlich. Aber wie gesagt zur Ergänzung Vorschläge habe ich schon am Anfang gegeben.

Jonathan Denzel: Würdest du sagen, die Projektvorlage bietet genügend Inhalt und Informationen, die Arbeitspakete zu strukturieren und die zu erledigenden Aufgaben anzugehen?

Markus Hefler: Ja, es ist ein sehr guter Leitfaden. Natürlich, von Projekt zu Projekt wird man da vielleicht unterschiedlich clustern, aber es ist auf jeden Fall eine gute Leitlinie, eine gute Hilfe. Definitiv.

Jonathan Denzel: Inwieweit würdest du der folgenden Aussage zustimmen? Die Umsetzung aller Arbeitspakete wird ein konsistent hohes Niveau der Cyber Resilienz in einer Organisation schaffen? Welche Faktoren beeinflussen da deine Entscheidungen, wenn du dazu ein Statement gibst?

Markus Hefler: Auf die erste Frage hin geantwortet, ja, auf jeden Fall. Und auf die zweite Frage. Ja, hängt ganz stark vom bestehenden Sicherheits- bzw. Resilienzniveau des jeweiligen Unternehmens ab. Man kann das keinesfalls über einen Kamm scheren. Für ein Unternehmen ist die Umsetzung wesentlich schwieriger als fürs andere. Also ich traue mir da ehrlich gesagt keine andere Antwort zu geben, weil es ganz stark unterschiedliche Niveaus gibt.

Jonathan Denzel: Jawoll. Du kennst dich ja mit der Dora schon aus. Inwiefern hast du den Eindruck, dass die Umsetzung aller Arbeitspakete die Erfüllung der Anforderungen gewährleisten wird?

Markus Hefler: Also wenn man die Arbeitspakete wirklich zu 100% umsetzt, so wie du es beschrieben hast, dann könnte man ein DORA Audit, wenn es gleich nach dem 17. Januar 2025 stattfinden soll, sicher positiv überstehen.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Jonathan Denzel: Vielen Dank. Und jetzt noch die offene Frage: Hast du sonst noch Feedback zu dieser Projektplanvorlage, die du noch nicht vorne während dem Durchgehen angesprochen hast?

Markus Hefler: Zusätzlich zu dem, was ich schon gesagt habe... Wie gesagt, die Clusterung, das ist halt ein bisschen Geschmackssache, muss man ganz ehrlich sagen, oder wie feinteilig man das clustern möchte. Weil hängt auch wieder von den handelnden Personen ab, wenn man eine eigene BCM-Abteilung hat, wird man ein bisschen anders clustern, als wenn alles unter der Cybersecurity Abteilung zusammengefasst ist oder was auch immer aufgehängt ist. Aber für die Arbeit und die Clusterung finde ich voll okay.

Jonathan Denzel: Vielen Dank. Dann sind wir mit dem offiziellen Teil durch.

C.2 Expert Interview 2

The following conversation was held between Jonathan Denzel and Markus Endres on 20th December 2023 via remote video call in German.

C.2.1 Transcript

Markus Endres: Bin wieder da.

Jonathan Denzel: Sehr gut. So. Dann starten wir. Purpose ist klar von dem Interview. Es geht um meine Evaluation von der Masterarbeit. Was die Vertraulichkeit angeht, ich nehme die Session auf und du kannst, ich schicke dir das Transkript zu und dann kannst du noch ändern, was auch immer du ändern möchtest, innerhalb von zwei Wochen.

Markus Endres: Okay.

Jonathan Denzel: Wenn du das möchtest, können wir deinen Namen anonymisieren oder die Beziehung zu Organisationen.

Markus Endres: Das sage ich dir, nachdem ich Transkript gelesen habe. Okay?

Jonathan Denzel: Jawoll. Du kannst auch jetzt, falls du noch Fragen hast zu dem Interviewprozess, noch Fragen stellen. Ansonsten Feedback kannst du auch noch nachträglich per Mail oder mir direkt geben.

Markus Endres: Passt.

Jonathan Denzel: Sehr gut. Die ersten zwei Fragen sind allgemein noch nicht bezogen auf das Dokument. Das erste ist nochmal an dich. Kannst du nochmal einen Überblick über deinen beruflichen Hintergrund, insbesondere auf das Management von IKT-Projekten, geben?

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Markus Endres: Ja, beruflicher Hintergrund ist , grundlegend komme ich aus dem Risikomanagement, Risikomanagement im Bankenumfeld, habe in dem Konnex einige Zeit in der Beratung im Risikomanagement für Banken gearbeitet, auch ein paar Jahre in der OeNB in der Bankenaufsicht für signifikante Banken. Bin dann als Chief Risk Officer und Chief Information Security Officer in einer der größten österreichischen Privatbanken gelandet. Habe das eben vier Jahre gemacht und danach eben gemeinsam mit den Kollegen Certitude gegründet, wo wir ja nichts anders machen, wie eben IKT-Projekte beziehungsweise Informationssicherheitsprojekte für Kunden abwickeln oder halt gestalten.

Jonathan Denzel: Jawohl, danke dir. Die nächste Frage ist, was ist aus deiner Sicht, was sind die Kernelemente für einen effektiven Projektplan?

Markus Endres: Das im Wesentlichen, dass einerseits die Projektplanung klar definierte Arbeitspakete hat, das klar ist, was ist bei den einzelnen Arbeitspaketen, was ist der Soll-Output, bzw. was ist das Ziel jeweils des Arbeitspakets bzw. was ist das Arbeitsergebnis und dann weiter klar muss auch dementsprechend mit dabei definiert sein, was sind dafür notwendige Ressourcen. Was sind die entsprechend festgelegten Timelines, also Deadlines. Ja, das sind so die wesentlichen Punkte, um dann eben das Projekt auch steuern zu können.

Jonathan Denzel: Okay. Dann die nächsten Fragen, da geht es um das Dokument und ich kann dich da hier durchführen oder du schaust selber einfach schnell über deines drüber. Das dürfte wesentlich schneller gehen.

Markus Endres: Ab welcher Seite ist dann das Relevante? Also ab Anhang B oder?.

Jonathan Denzel: Ja genau ab Anhang B, richtig.

Markus Endres: Was ist dann, was ist die Frage, damit ich weiß, was gefragt wird, bevor ichs mir durchschaue?

Jonathan Denzel: Jap. Also es geht um welche Abschnitte davon besonders wertvoll sind und warum, inwiefern das Format und der Inhalt leicht verständlich sind, ob die Form zweckmäßig gewählt wurde, ob es ein anderes Format geben würde, was es verbessert, ob die Arbeitspakete klar definiert sind und die Ziele davon, ob die KPIs zweckmäßig und messbar sind. Das sind so die Detailfragen. Dann kommt noch ne Frage zu Projektrisiken und danach nur noch wie du das insgesamt bewertest.

Markus Endres: Okay. wie man sieht, du hast jetzt hier auf Seite 6 und 7 dementsprechend das Template beschrieben und dann eigentlich diese Working Packages, die hast du dann ab Seite 8, oder?

Jonathan Denzel: Genau, ja. Also es geht eben zuerst in diesem Projekt-Frame, was so das grobe Projekt umreißt, wann geht's los was ist das Budget insgesamt an

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Manntagen und an zusätzlichem Geld. Wer ist alles beteiligt, was ist die Deadline, welche Meetings finden wiederholt statt; dann die KPI die man währenddessen erheben könnte über so ein Projekt; die Projektrisiken, da habe ich drei identifiziert: Knappheit von Ressourcen, eine Lücke zwischen Dokumentation und Implementierung und eine Resistenz gegenüber Änderungen. Wo ich sage das erste Risiko braucht ein klares Commitment vom Management und die involvierten Personen müssen ihren Day-to-Day Workload reduzieren. Dann um diese Gap zwischen Dokumentation und Implementierung angehen zu können, braucht es auch da wieder genügend Ressourcen um es tatsächlich umzusetzen. Und um die Resistenz gegen Veränderungen zu überwinden, braucht es ein klares Statement vom Management, es muss eine hohe Priorität im Unternehmen haben und angepasst sein auf den individuellen Kontext der Organisation.

Markus Endres: Okay. Der Projektplan ist eben aber auch das mit den Arbeitspaketen. Oder?

Jonathan Denzel: Genau, aber da gehört zu jedem Paket diese fünf Zeilen direkt oben drin, wann gehts los, wann soll es fertig sein, wer ist der Task-Owner, wer sagt: Jetzt gehts los, wer sagt: Jetzt sind wir fertig?

Markus Endres: Okay.

Jonathan Denzel: Und dann gehts in die einzelnen Arbeitspakete rein.

Markus Endres: Und die gehen dann bis zum Ende oder?

Jonathan Denzel: Die gehen dann bis zum Ende.

Markus Endres: Gut, und was hast du denn da für Fragen jetzt dazu?

Jonathan Denzel: Also die, die wir bisher schon klären können ist: welchen Abschnitt oder Aspekt des bereitgestellten Dokuments hältst du aus deiner Sicht für besonders wertvoll und warum? Ah, soll ich nochmal über alle gehen oder?

Markus Endres: Ich meine, Teil des Plans ist, es gibt im Wesentlichen nur zwei, es gibt dieses Template und dann gibt es ja dieser Rahmen eigentlich mehr oder weniger, meine ich, was du jetzt beschrieben hast. Und dann gibt es ja die einzelnen Arbeitspakete, diese beiden Teile gibt es, oder? Oder möchtest du wirklich auch wissen, ob ich jetzt ein Arbeitspaket für sich gesehen als wertvoll empfinde?

Jonathan Denzel: Ich würde es jetzt nicht nur in zwei Teilen sehen, sondern diesen Rahmen auch aus einzelnen Teilen und dann vielleicht zwischen diesen einzelnen Teilen und den Arbeitspaketen. Wie du das für wertvoll erachtest?

Markus Endres: Etwas das sicher wertvoll ist, immer wenn du es hast, ist einerseits klar, dass du diese KPI definierst zum Projekt, dass du dementsprechend dann auch

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Projektfortschritt und auch Projektumsetzung messen kannst. Und natürlich auch, dass du dementsprechend Projektrisiken und auch die Mitigation dazu eben definiert hast, das ist sicher wertvoll. Der Projektrahmen, dass du das vorgibst. Das sind sicher alles Punkte, die wesentlich sind bei einem Projekt oder bei einer Projektplanung. Und auch dann natürlich die Arbeitspakete per se - ohne die hast du eh kein Projektplan - insofern, ja, ich wüsste jetzt nicht, welcher Teil davon jetzt nicht wertvoll ist. Ehrlich gesagt.

Jonathan Denzel: Okay, ja. Hältst du das Format von dem Dokument für leicht verständlich?

Markus Endres: Naja, das ist halt, wie gesagt, das Format ist halt etwas, was man als Projektdokumentation verwenden kann. Im Projektmanagement selber ist das Format jetzt nicht zweckdienlich. Also, wenn du jemand zeigen willst, dass du alles super mit dokumentierst, was du ihnen geben kannst, dann wäre sicher so was. Aber jetzt fürs Projektmanagement selber und dann auch natürlich das, dass jeder damit arbeiten kann und das Projekttracking nach haben und so ist das natürlich nicht das. Also ist so ein Format dann nicht das klassische Format, weil du siehst ja auch dort, die Definition der einzelnen Pakete, aber was du brauchst, viel mehr brauchst, ist ja entsprechend jetzt Gesamtübersicht über diese einzelnen Arbeitspakete mit den Zeitleisten, mit den auch Verknüpfungen untereinander, wie die Abhängigkeiten sind und so weiter und so fort.

Jonathan Denzel: Okay, ja.

Markus Endres: Wo ich jetzt auch nicht weiß, was das Ziel ist von dem Dokument per se ist, für dieses Dokument ist.

Jonathan Denzel: Es soll als Orientierungshilfe gehen für Organisationen, die jetzt ein DORA-Projekt angehen möchten. Dass Sie sich da als Leitfaden orientieren können.

Markus Endres: Okay. Naja, für so was ja. Der Projektplan per se was du hier hast, das ist die Basis für den Projektplan. Der Projektplan ist natürlich immer sehr stark mit, oder was ganz wesentlich ist, beim Projektplan sind: dass du jeweils dann sagst, was sind jetzt die einzelnen Arbeitspaketen, was ist der Projektbeginn, was ist das Projektende. Also wann startet es und was ist dementsprechend die Deadline. Und vor allem auch, dass du eben siehst untereinander die Abhängigkeiten, also welches Projektpaket musst du vorher machen, was kommt danach, wie hängen die miteinander in Verbindung, das ist ganz wesentlich. Das hättest hier halt nicht klar. Beziehungsweise vielleicht ist es im Text drinnen. Aber das braucht man halt eher sicher im Projekt selber noch. Das muss etwas plastischer vor sich sieht und nicht immer nachlesen muss.

Jonathan Denzel: Zu den KPI, die definiert sind, sind die einfach zu verstehen, zweckmäßig und messbar?

Markus Endres: Ah... die on time completion percentage ... Ja, stimmt schon... Das KPI das jetzt sicher nicht schlechter wäre ist als Kennzahl hast, was generell so

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

der Projekt-Umsetzungsstand ist. Also den Prozentsatz von bereits Umgesetzten, bzw. wie viel Prozent, man vom Gesamten schon umgesetzt hat, oder? Oder hättest du das irgendwo mit drin, ich hab's überlesen.

Jonathan Denzel: Ja stimmt. Ja die Burndown-Rate, aber das ist auch nicht ganz das.

Markus Endres: Ja aber warte mal... Weil das mit den Workingpackages ... ist auch nicht ganz hundertprozentig. Dann habe ich vom Gesamtprojekt, also bzw. von den einzelnen Arbeitspaketen und dann eben vom Gesamten, bin ich jetzt bei 10 % oder bin ich bei 95 % von der Umsetzung, das ist sicher mal etwas, was Sinn machen würde, aber sonst, also grundsätzlich, ja, sind verständlich, was du da hast.

Jonathan Denzel: Danke. Bietet das Dokument einen klaren Gesamtüberblick und einen nützlichen Handlungsleitfaden zur Umsetzung von Cyberresilienz-Projekten für Organisationen?

Markus Endres: Ist es das Ziel von dem, weil ich dachte es ist für DORA?

Jonathan Denzel: Es ist am Ende, wenn du die DORA umgesetzt hast als Organisation auch ein gewisses Maß an Cyberresilienz aufgebaut. Das ist ja das Ziel von der DORA dann wieder.

Markus Endres: Also ja, wie gesagt, so gesehen wahrscheinlich schon. Das ist dann halt so umgesetzt, wie das DORA vorsieht, aber ja. Mhm. Also ja.

Jonathan Denzel: Okay. Sind die Arbeitspakete und Ziele klar definiert? Da geht es jetzt in die Arbeitspakete rein. Vielleicht schaust du die dir mal ein bisschen an.

[Markus Endres blättert das Dokument durch]

Markus Endres: Beim Incident Management hast du ja z.B. als Input, die Strategie, die Beschreibung ist kurz und das Ziel ist halt, dass ein „documented process identifies, treats and prevents ICT related incidents". Ich meine, da wäre jetzt für mich die Frage noch, und es sind ja sehr viele Sachen auch, und wenn ich jetzt, also unabhängig von DORA, wenn ich das jetzt mit DORA mache, dann sind es ja sehr viele Sachen auch die klar vorgegeben sind, was im Rahmen dieses Prozesses alles berücksichtigt sein muss. Das wüsste ich jetzt hier nicht.

Jonathan Denzel: Also der Detailgrad fehlt.

Markus Endres: Genau, aber hier steht ja nur, oder auch bei anderen Dokumenten, ich habe das mit der Approved Business Continuity Guideline, okay, ist schön, aber was sind die Inhalte von dieser Business Continuity Guideline. Das könntest jetzt haben in der Beschreibung? Wenn die Beschreibung etwas umfangreicher wäre, dann könnte man es daraus nehmen und sagen, okay, das muss drinnen sein. Oder zumindest, was sind die

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

wesentlichen Inhalte, die wesentlichen Themen, die es dort behandelt haben musst? Dann wird das mit Objective wahrscheinlich ausreichen. Aber ansonsten muss das wirklich auch im Objective, im Ziel nach und festlegen, was ist wirklich so die Mindestinhalte, die auch da... angemessen abgehandelt sein müssen im Rahmen des Testens. Das wird hier, das wird sicher fehlen, weil da müsste es dann, dieses hast, dieses Arbeitspaket, dann müsstest nochmal in der DORA Guideline oder vielleicht in anderen Dokumenten nachschauen, was ist da alles mit umfasst in diesem Thema. Also was müsste alles mit umfasst sein?

Jonathan Denzel: Ja. Verstehe. Jetzt geht es nochmal auf die Projektrisiken, die wir vorher angesprochen hatten. Sind die identifizierten Risiken, decken die sich mit deinen Erfahrungen aus der Vergangenheit im Bezug auf Projektfehler oder Projektrisiken?

Markus Endres: Ja, ich meine einerseits diesen Punkt mit Ressourcen, das ist natürlich ein billiges Risiko, weil das ist natürlich immer ein Risiko, dass du zu wenig Ressourcen dafür hast, das ist klar. Gap between documentation, implementation, die hat man vielleicht nicht so oft, aber ja, ist ein Risiko, das passt sicher. Ja hinsichtlich der resistance to change, auch das, ja. Das ist ein Risiko, was immer besteht und was entsprechend adressiert sein müsste oder muss. Wo bei DORA jetzt sicher mit aufnehmen können als Risiko, dass auch die konkrete Ausgestaltung noch nicht hundertprozentig abgeschlossen oder festgelegt ist, weil da auch noch gewisse Dokumente zumindest noch finalisiert werden müssen oder eben dementsprechend noch nicht hundertprozentig ausgearbeitet sind. Das ist sicher etwas, was du mit aufnehmen hättest können. Beziehungsweise vor allen Dingen bei den Ressourcen selber... Die Frage ist, ob ich jetzt nur die personellen Ressourcen oder auch andere Ressourcen adressiere. Ja, personell. Also wie gesagt, es können einerseits auch andere Ressourcen sein, wie nur personelle Ressourcen, weil möglicherweise auch damit natürlich andere Kosten oder andere Notwendigkeiten verbunden sind. Beziehungsweise ist natürlich auch da, was ich auch mit dem Risiko wäre, ist Ressourcen nicht nur bei dir, sondern auch bei Dritten. Vor allem wenn du die Drittdienstleistern anschaust, bzw. auch, glaube ich, was sicher ein Risiko wäre, was beleuchtenswert ist, ist, dass du Probleme hast, die notwendigen Inputs, aber auch die notwendigen Tätigkeiten von den Drittdienstleistern entsprechend zu bekommen. Also denkt mal an die [Erwähnung eines gemeinsamen Projekts in einer Bank] zum Beispiel, da ist jetzt mal schon die Frage, ob die Drittdienstleister wesentlich auch mitspielen bei dem ganzen Thema. So was ist doch ein Risiko, was natürlich mit dabei sein könnte oder sollte.

Jonathan Denzel: Ja. Stimmen die Strategien zur Risikominimierung? Würdest du sagen, die sind richtig getroffen?

Markus Endres: Ah, hat beim ersten... Am Ersten ist es ein Satz zu Commitment. Ja, das ist wichtig, was sicher auch da ist, um das zu minimieren, ist, dass man das Projekt sehr eng auch tracked und reportet. Weil ich glaube, bei Ressourcen ist man richtig am Anfang, aber es ist wichtig, dass man auch die notwendigen Ressourcen, die man so

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

einschätzt, bekommt. Aber dann ist es umso wichtiger, dass man dann auch immer nach Zeiten anschaut, dass die Ressourcen entsprechend dabei der Ressourcenbedarf bleibt, ist er meistens nicht so wie man ihn plant bzw. kann er sich laufend ändern. Und da muss man einfach sehr viel Transparenz haben und auch dann immer wieder berichten, auch zeitnah, dass man auch sieht, okay, sind jetzt immer noch notwendige Ressourcen da oder ist es dementsprechend, geht das Projekt so voran, wie es vorangehen müsste und dass man hier das sicherstellt, dass eben auch während der Projektlaufzeit notwendige Ressourcen bereitgestellt werden. Es ist aber auch wichtig, nicht nur, dass man einmal das Management entsprechend commited hat, sondern dass das laufend da ist und das läuft auch nur über Transparenz und Berichterstattung. Mit der Einbindung.

Beim zweiten. Ich glaube, es ist nicht nur das, dass man nur die internen Ressourcen hat, sondern dass die entsprechend auch die internen klarerweise dabei sind selber. Dass man von Anfang an auch genügend Ressourcen vorsieht, um diese Implementierung auch möglich zu machen überhaupt. Nur, dass die eingebunden sind - wenn sie dann dafür keine Zeit haben, das operativ umzusetzen, bringt es nichts, dass sie dabei sind. Wichtig ist, dass sie dabei sind und eben auch die Möglichkeit haben, dann überhaupt das umzusetzen.

Change... das passt.

Jonathan Denzel: Okay. Danke dir. Inwiefern würdest du sagen, der Inhalt der Projektplanvorlage bietet ausreichend Information um die Arbeitspakete zu strukturieren?

Markus Endres: Wie viel der Plan, genügend Input liefert, um die Arbeitspakete zu strukturieren? Wenn man davon ausgibt, dass die Sachen da sind, die da drinnen stehen, Start, Datum, also bei jedem Paket wäre das Startdatum ist da die Deadline ist da, der Owner ist da. Ja, es ist ja quasi, hier eben zu strukturieren wirklich fehlen würde noch, das einzige, was wesentlich fehlt, ist die Abhängigkeit der einzelnen Arbeitspakete untereinander. Okay. Das fehlt dir.

Jonathan Denzel: Ja ok. Dann...

Markus Endres: Ich würde sagen, grundsätzlich muss man sagen, rein um diese Startdatum, Deadline zu bestimmen, brauche ich die Abhängigkeit. Wenn jetzt das schon da ist, dann könnte man rein theoretisch darauf verzichten, oder dann müsste jeder davon ausgehen, dass eben die Startdatum von Paketen so ist, dass es mit den Deadlines von den Sachen, die ich brauche, eben abgestimmt ist. Aber, weil um diese Punkte hier, das Startdatum und Deadline, bestimmen zu können von den Dingen, ist als erstes im ersten Schritt mal wesentlich die Abhängigkeiten zu wissen untereinander.

Jonathan Denzel: Ja, nehme ich mit. Dann kommen wir zu den Schlussfragen. Die erste ist die Umsetzung aller Arbeitspakete wird in konsistente,...

Markus Endres: Beziehungsweise zusätzlich vielleicht noch ein zweiter Punkt, weil du es hier mit dem Task Owner, der ist das wesentlich aber, wo es auch noch notwendig ist,

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

dass man nicht nur den Owner weiß, sondern auch eben wer aller sonst noch Mitarbeiten muss dabei, wenn anderen Bereich Abteilung man dazu braucht.

Jonathan Denzel: Okay, ja, auch das.

Markus Endres: Ja, na dann, was ist die nächste Frage?

Jonathan Denzel: Die nächste Frage ist, inwieweit stimmst du der folgenden Aussage zu? Die Umsetzung aller Arbeitspakete wird ein konsistent hohes Niveau der Cyberresilienz innerhalb einer Organisation schaffen. Und welche Faktoren beeinflussen dabei deine Entscheidung? Wenn du sagst, du stimmst die Aussage zu oder eher nicht.

Markus Endres: Die Umsetzung dieser Maßnahmen, ein hohes Maß an Cyberresilienz gewährleistet?

Jonathan Denzel: Genau.

Markus Endres: Ja, wenn man alles umsetzt, die wirklich alle Themen auch in dem Detailgrad, wie sich die DORA vorsieht, best practice umsetzt, wenn man das best practice umsetzt, dann hat man so ziemlich, man hat sehr viel, was die Cyberresilienz beeinflusst, hat man dann entsprechend umgesetzt. Ich glaube, ich finde es wichtig, diese Pakete, die einzelnen Arbeitspakete best practice umsetzt, dann ja.

Jonathan Denzel: Okay. Perfekt. Und...

Markus Endres: Das umsetzt irgendwie dann.

Jonathan Denzel: Da spiele ich vielleicht die letzte Frage drauf an. Inwieweit hast du den Eindruck, dass die Umsetzung aller Arbeitspakete die Erfüllung der Anforderungen nach DORA gewährleisten wird?

Markus Endres: Ich gehe davon aus, dass du da alles drin hast. Ich schaue mal ganz kurz an. [...] ich gehe davon aus, dass du das da alles abdecken solltest. Wenn ich so drüber schaue glaube ich, dass wir recht vollständig sind. Es würde mir nichts auffallen, was wirklich fehlen würde.

Jonathan Denzel: Perfekt.

Markus Endres: Also auf die Überschriftenebene.

Jonathan Denzel: Mhm. Und die letzte Frage ist, willst du sonst noch Feedback, das du noch nicht angebracht hast, jetzt hinzufügen?

Markus Endres: Nah.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Jonathan Denzel: Gut.

Markus Endres: Ich hab dir alles gesagt, was ich, was mir dazu einfällt, deswegen nein, also von dem her.

Jonathan Denzel: Passt.

C.3 Expert Interview 3

The following conversation was held between Jonathan Denzel and Michael Clauss on 14.01.2024 via remote video call.

C.3.1 Transcript

Jonathan Denzel: Guten Tag Herr Clauss. Vielen Dank dass sie sich bereit erklärt haben an dem Experteninterview teilzunehmen.

Michael Clauss: Sehr gerne.

Jonathan Denzel: Ich führe im Rahmen meiner Masterarbeit diese Experteninterviews durch. Es geht um die schrittweise Implementierung von Maßnahmen zur Cyber-Resilienz. Ich würde das Audio mit meinem Handy aufnehmen und dann vertraulich in meinem Archiv aufbewahren und nur zur Transkription verwenden. Das Transkript stelle ich Ihnen vor der Veröffentlichung zur Verfügung und Sie können innerhalb der nächsten vierzehn Tage nachdem ich es Ihnen zugeschickt habe Änderungen daran vornehmen. Wir können auch ihren Namen oder die Assoziation zu Organisation entfernen, sofern Sie das im Nachgang wünschen. Passt das für sie?

Michael Clauss: Ja das passt.

Jonathan Denzel: Sehr gut. Kommen wir zur ersten Frage. Könnten Sie einen kurzen Überblick über Ihren beruflichen Hintergrund und Ihre Erfahrungen im Bereich des Managements von IKT-Projekten geben?

Michael Clauss: Gerne. Ich bin seit 2017 länderübergreifend verantwortlich im Unternehmen Airbus Defence and Space für die Einhaltung produktbezogener gesetzlicher Vorschriften, wozu auch die Einführung von IT-Lösungen gehörten, z.B. SaaS (Software as a Service) für das Regulations & Requirment Management oder Werkzeuge für das Material Compliance Reporting mit Anbindungen an die SAP Systeme (PLM, ERP) von Einkauf, Entwicklung, Produktion und Logistik. Davor habe ich firmenübergreifend die Funktion Risikomanagement für alle Programme und Funktionen des Unternehmens geleitet.

Jonathan Denzel: Der nächste Punkt geht allgemein um Projektpläne. Was sind da aus ihrer Sicht Kernelemente für einen effektiven Projektplan?

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Michael Clauss: Ein effektiver Projektplan erfordert erst einmal ein klares unternehmensweites Planungsmandat, eine Benennung der Sponsoren und Sicherstellung deren effektiven Unterstützung im Bedarfsfall. Dann braucht ein Projektplan eine klare Struktur, idealerweise in Form eines Netzplans, der Hierarchien und Verbindungen zwischen den Projektteilen aufzeigt. Weiter ist es hilfreich, die Abhängigkeiten zwischen den einzelnen Aktivitäten klar darzustellen, insbesondere welche Aufgaben Vorläufer und welche Nachfolger sind.

Von Bedeutung ist auch die Erkennbarkeit der wesentlichen Meilensteine, die mit dem Kunden vereinbart werden. Zur Planung hilft eine Darstellung des kritischen Pfades, da diese die Gesamtprojektlaufzeit bestimmt.

Die Zuordnung von Aktivitäten zu spezifischen Arbeitspaketen und Verantwortlichen hilft, die Organisation und Verantwortlichkeiten klar zu definieren.

Dann ist es noch wichtig, Anfang, Dauer und Ende jeder Aktivität genau zu planen und dabei ausreichende Pufferzeiten einzuplanen, um einen realistischen Terminplan zu gewährleisten. Denn es müssen die Dauer der Aktivitäten unter Berücksichtigung der Verfügbarkeit der Ressourcen, wie beispielsweise geplante Abwesenheitszeiten, Teilzeitverfügbarkeiten oder Urlaub der Mitarbeiter, realistisch geplant werden.

Jonathan Denzel: Soweit ihre Einschätzung das sind sicher viele wichtige Aspekte dabei. Dann kommen wir jetzt auf das Dokument, dass ich Ihnen im Vorfeld geschickt habe zu sprechen. Welche Teile davon empfinden Sie als besonders wertvoll und warum?

Michael Clauss: Die vorgestellte Vorlage des Projektplanes hat einen Schwerpunkt im kritischen Bereich des Third Party/Outsourcing und Risk Managements, deren Bewertung und Verbesserung ein wichtiges Projektziel darstellt. Damit ist ein wichtiger Aspekt der Verbesserung der Cyber-Resilienz aufgegriffen worden.

Jonathan Denzel: Wie würden Sie das Format und den Inhalt einordnen? Sind diese leicht zu verstehen?

Michael Clauss: Ihre Projektplanvorlage ist verständlich niedergeschrieben und würde direkt anschließen, dass das Dokument auch zweckmäßig und nützlich ist.

Jonathan Denzel: Sehr gut. Dann als nächstes die Arbeitspakete. Sind diese und die Ziele der Arbeitspakete klar definiert?

Michael Clauss: Ja. Ich würde sagen die aufgeführten Arbeitspakete decken thematisch alle wesentlichen Elemente zur Sicherung der Cyber-Resilienz ab. Inhaltlich und in der Zielbeschreibung finde ich die Pakete klar beschrieben. Für ein konkretes Projekt muss der Detaillierungsgrad sicher noch gesteigert werden.

Jonathan Denzel: Ja das sicherlich. Wie steht es aus ihrer Sicht um die KPI, die am Beginn des Templates formuliert sind? Empfinden Sie diese als verständlich, zweckmäßig und einfach zu messen?

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Michael Clauss: Die aufgeführten KPIs sind zweckmäßig aber nicht immer leicht messbar (z.B. Number of Adjustments) bzw. nicht sehr aussagefähig (z.B. Team Members leaving vs. joining the Project after Initiation). Als weiteren aussagefähigen KPI schlage ich noch vor, neben der WP completion percentage die Milestones Adherence mitzuverfolgen sowie ein kontinuierlich gepflegtes Risk- und Opportunity Register im Projekt zu führen, um Trends frühzeitig im Projektverlauf zu identifizieren und gegenzusteuern.

Jonathan Denzel: In wie weit bietet das Dokument einen klaren Gesamtüberblick und einen nützlichen Handlungsleitfaden zur Umsetzung von Cyber-Resilienz-Projekten für Organisationen?

Michael Clauss: Die vorliegende Masterarbeit beschreibt aus meiner Sicht einen systematisch aufgebauten, umfassenden Massnahmenkatalog zur Umsetzung von Cyber-Resilienz-Projekten. Als solchen kann er als nützlicher Startpunkt und Leitfaden für Unternehmen dienen um damit auch gleichzeitig die DORA-Compliance aufzubauen und zu dokumentieren.

Jonathan Denzel: Im nächsten Teil geht es um die am Anfang beschriebenen Projekt Risiken. Stimmen diese Risiken mit den Risiken überein, die Sie in der Vergangenheit in Projekten erlebt haben?

Michael Clauss: In meiner Vergangenheit hat sich in diversen IKT-Projekten gezeigt, dass alle wesentlichen Stakeholder frühzeitig und umfassend bezüglich Ihrer Erwartungshaltung in ein solches Projekt eingebunden werden müssen. Ich sehe da vor allem das Stakeholder Expectation Management und voice of the internal customer. Damit nicht am Bedarf vorbei Lösungen entwickelt werden. Dabei kann bereits ein relativ simples mapping helfen: What is in? vs. What is out? Außerdem ist durch den firmenübergreifenden Charakter von Cyber Security Projekten ein sehr robuster Entscheidungsprozess im Projektverlauf sicherzustellen.

Jonathan Denzel: Inwieweit sind die Strategien oder Lösungen zur Risikominierung korrekt und nützlich?

Michael Clauss: Die kritischen Aspekte für eine erfolgreiche Projektumsetzung sind erfasst und die vorgeschlagenen Maßnahmen zur Risikominimierung sind zutreffend.

Zur Absicherung der Verfügbarkeit von Schlüsselpersonal ist neben des Management-Commitments auch das persönliche Commitment jedes Teammitglieds zum eigenen Projektbeitrag sowie ein gutes Teambuilding von Beginn an wichtig. Sichtbarkeit der eigenen Beiträge z.B. im Steering committee / Steuerkreis können einen motivierenden Faktor darstellen ebenso wie das „Feiern“ von erreichten Meilensteinen. Um eine gute Dokumentation sicherzustellen, muss im gesamten Projektverlauf großer Wert auf kontinuierliche Qualitätskontrolle durch Reviews gelegt werden. Die Freigabe der Dokumentation eines Arbeitspaketes ist als Deliverable festzulegen.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Ist in der Projektplanung bereits erkennbar, dass etablierte Geschäftsprozesse angepasst werden müssen, hat sich die Einrichtung eines projektbegleitenden Arbeitspaketes „Change Management“ mit Elementen von Kommunikation und Schulung der betroffenen Mitarbeiter bewährt. Dafür sind terminliche und Ressourcen-bezogene Vorkehrungen einzuplanen.

Jonathan Denzel: Ja. Das sind sicher auch wichtige Punkte, die nehm ich so mit. Kommen wir nun nochmal zum Inhalt. Bietet die Vorlage ausreichend Informationen um die Arbeitspakete zu strukturieren und ein klares Verständnis der Aufgaben zu erhalten?

Michael Clauss: Mit den vorgeschlagenen insgesamt 52 Arbeitspaketen eingeteilt in die 3 Kategorien „Organisational Governance“, „IT Controls“ und „Technical Implementation“ wird das Template des Projektplanes den Anforderungen an Umfang, Strukturiertheit und Vollständigkeit gut gerecht. Insbesondere zeigt sich beim Mapping mit den legalen Anforderungen der DORA aus meiner Sicht die Vollständigkeit der Compliance-Absicherung.

Jonathan Denzel: Da sprechen Sie auch schon direkt die Compliance mit DORA an. Aber vorher noch würden Sie zustimmen, dass die Umsetzung aller Arbeitspakete ein konsistent hohes Niveau der Cyber-Resilienz innerhalb einer Organisation schaffen? Und wie würden Sie ihre Einschätzung begründen?

Michael Clauss: Die Zielsetzung der DORA-Regulierung besteht darin, dass sich Unternehmen systematisch mit den real vorkommenden Cyber Threats und den damit konkret für Unternehmen verbundenen Geschäftsrisiken ausseinandersetzen, das gilt ja nicht nur für Unternehmenungen der Finanzbranche sondern in besonderem Maße auch für High-Tech Unternehmen wie Airbus Defence & Space. Daher führt eine umfassende Compliance-Absicherung gegenüber DORA-Anforderungen auch immanent zu einer Verbesserung der Cyber-Resilienz in der betreffenden Organisation oder Unternehmen. Für ein kontinuierlich hohes Niveau der Cyber-Resilienz sind gegebenenfalls fortlaufend weitere organisationsspezifische Massnahmen notwendig.

Jonathan Denzel: Das ist die Übereinstimung von tatsächlicher Resilienz mit den Compliance Anforderungen. Dann doch noch mal nach der Compliance gefragt. Wieweit wird ihrer Ansicht nach die Umsetzung aller Arbeitspakete die Anforderunge der DORA Anforderungen erfüllen?

Michael Clauss: Grundsätzlich ist es für die Compliance eines Unternehmens insbesondere bei neuen regulativen Anforderungen wichtig, diese neuen Regularien zu kennen und sich ein klares Bild davon zu machen, ob und in welchem konkreten Umfang diese regulativen Anforderungen für das eigene Unternehmen anzuwenden sind. Also eine Awareness und eine Fit-Gap-Analyse durchzuführen. Sobald festgestellt ist, dass das eigene Unternehmen ganz oder teilweise betroffen ist, ist ein Plan zu erstellen, wie die identifizierten Lücken zu schließen sind. Zu diesem Zweck ist der in der Masterarbeit vorgestellte Projektplan inklusive der notwendigen Arbeitspakete sehr gut geeignet,

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

gegenüber Vollzugsbehörden die eigenen Compliance-Bemühungen in einer strukturierten Form darzustellen. Mit dem festen Committment des Managements, einer ausreichenden Ressourcen-allokation und dem Start eines Projektes gemäß dem vorgestellten Projektplan kann sich ein Unternehmen bereits von einer vorsätzlichen beziehungsweise grob fahrlässigen Non-Compliance befreien.

Jonathan Denzel: Dann haben wir es schon fast geschafft. Zum Schluss noch. Gibt es sonst noch Feedback, dass Sie zum Template, der Masterarbeit oder dem Interview abgeben möchten?

Michael Clauss: Als wichtige Projekt Parameter sollten zusätzlich zu den bereits aufgeführten erfahrungsgemäß noch folgende Parameter genannt sein. Steering Board Members, Accountable Manager (der für die Umsetzung Zuständige), das unterschriebene Management Commitment für die Schlüsselressourcent und zusätzlich zur beschriebene Deadline (=Project Closure) auch die Major Milestones

Außerdem ist im sonstigen Teil der Masterarbeit die Sie mir auch zugeschickt haben neben der sehr hilfreichen Ausarbeitung und Literaturanalyse von Anforderung und operationellen Leitfäden das Kapitel 6 “Design Verification against Requirement” sehr nützlich. Mit dem Mapping von gesetzlichen Forderungen und vorgeschlagenen Arbeitspaketen, die diese inhaltlich abdecken kann sowohl intern als auch bei externen Audit oder Überwachungen gut die Compliance gegen legale Anforderungen dargestellt und abgesichert werden.

Jonathan Denzel: Nocheinmal abschließend vielen Dank für ihre Zeit. Dann sind wir mit dem Interview soweit fertig. Ich schicke Ihnen das Transkript alsbald zu.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

APPENDIX D

OeNB Interview on DORA

D.1 Purpose

The purpose of the interview is explained to the participant as follows: The interview deepens the understanding regarding DORA audits and the background of DORA for this master thesis.

D.2 Confidentiality

The audio of the interview will be recorded through either a mobile phone microphone or in the case of remote interviews through the recording of the session. The recordings are only used for transcription. The interviewee can withdraw or amend any answers given throughout the interview within two weeks after receiving the written transcription. The name of the interviewee and/or his association to any organisation can be excluded from the publication upon request.

D.3 Format

The format of the interview is the standardized open-ended interview. Within this format through either a remote conference or an in person interview the interviewee is asked a standardised set of questions upon which the interviewee can answer freely. The planned duration of each interview is 30 minutes. The interviewee has the possibility to send further feedback regarding the session per mail within two weeks from the interview. The interviewee has the possibility to ask questions before the interview begins.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

D.4 Prepared Questions in German

The interview with the Austrian National Bank is held in German. The following questions are therefor formulated in German. These question pose as a guideline for an expert interview with an open structure.

1. Gibt es innerhalb der OeNB einen Personalaufbau für DORA Prüfungen?
2. Inwiefern empfinden die Prüfer die Komplexität der Aufgaben als herausfordernd?
3. Wie bewerten Sie die Verhältnismäßigkeit als Teil der DORA, nachdem in vielen Themenbereichen sehr explizite aufwendige Maßnahmen gefordert sind (Beispiel: IKT-Drittanbieteraudits)? Sind diese auch in vollem Umfang für kleine Bankhäuser anzuwenden?
4. Wissen Sie heute schon, wie die Prüfungen der Banken bezüglich DORA aufgebaut sein wird? Stichprobenartig nach Themengebieten oder vollumfängliche Prüfung aller verpflichtenden Maßnahmen?
5. Eine grobe Einschätzung: Wie viel Prozent der Banken planen Sie pro Jahr zu prüfen?
6. Gibt es Toleranzen für Vorlaufzeiten, insbesondere im Zusammenhang mit aufwändigen technischen Maßnahmen?
7. In der DORA werden viele Aufgaben eines “Security Operations Center” gefordert. Ist die DORA dahingehend zu verstehen, dass alle Banken ein solches einkaufen oder betreiben müssen?

The interview is held in the OeNB main building on the 15th December 2023. The two participants are Jonathan Denzel as the interviewer and Stefan Unteregger as the interviewee. Stefan Unteregger is the Audit Manager in the Large Banks division, responsible for operational risk and IT risk, and currently coordinating the OeNB's DORA implementation activities.

D.5 Interview Transcription

Jonathan Denzel: Ich werde das Gespräch transkribieren und als Anhang noch mit reinpacken in meine Diplomarbeit. Vielen Dank. Die erste Frage ist zum Personalaufbau. Wird es im Kontext der DORA Personalaufbau geben in der OeNB?

Stefan Unteregger: Also nach derzeitigem Stand nicht. Nicht extra für DORA. Wie gesagt, im Hintergrund, die Ressourcen im Bereich IT Aufsicht sind über die letzten Jahre hinweg aufgebaut worden. IT-Risiko ist seit mehreren Jahren einer der strategischen Schwerpunkte in der Bankenaufsicht. Das war auch, was ich vorhin gemeint habe, dass das

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

eben jetzt keine neuen Themen mit DORA sind. Der Zweck von DORA fürs IT-Risiko ist es vor allem, dieses für Banken sehr wichtige Risiko, als explizit genannte Risikokategorie zu verankern, wo wir im bisherigen Bankaufsichtsrecht das operationelle Risiko hatten, wo das natürlich drin ist, weil ja Menschen, Prozesse, Systeme und externe Ereignisse, die vier Hauptkategorien im operationellen Risiko sind. Aber aufgrund der Bedeutung, die das Thema hat und dann jetzt auch im Zuge Digitalisierung und so, immer mehr in den Fokus gerückt ist, wollte man es nicht länger so als Unterkategorie operationelles Risiko dort mit gemeint haben. Und man wollte die Detailanforderungen im IT-Risiko, die vorher im europäischen Bankaufsichtsrecht nicht oder dann seit es die EBA-Guideline IT-Risk gab, zwar vorhanden, aber jetzt streng genommen nicht rechtlich bindend waren, auf ein rechtlich höherwertiges Fundament stellen. Und deswegen sind sehr viele Inhalte, die in DORA drinnen sind, gerade die sich an die Finanzinstitute richten, Inhalte, die wir vorher schon gefordert haben, vorher schon geprüft haben.

Jonathan Denzel: Über die EBA-Guideline?

Stefan Unteregger: Über die EBA-Guideline in einigen Ländern. Es gab auch in Österreich vor der EBA-Guideline kurz eine Richtlinie der Finanzmarktaufsicht zum IT-Risiko für Kreditinstitute. Die wurde da nur, weil sie jetzt ohnehin nicht viel was anderes ausgesagt hat, dass die EBA-Guideline im Geist der europäischen Harmonisierung, hat man gesagt, wir ziehen die Nationale zurück und verwenden die Europäische ab sofort. Aber sowohl die FMA-Richtlinie als auch die EBA-Guideline, waren eben streng genommen non-binding. Die FMA hat bestimmte Verordnungskompetenzen, aber die sind aufgrund österreichischen Verfassungsrechts sehr eingeschränkt. Das heißt, die FMA kann nicht einfach sagen:" Oh IT-Risiko! Wichtig! Wir machen jetzt eine bindende, verpflichtende-". Das wären dann österreichische Verordnungen der Behörde, die so was erlässt und das können die nicht machen. Was sie tun können, sind Interpretationen der allgemeinen Bestimmungen. Und im Paragraf 39 BWG steht drinnen, Banken - also der Vorstand - ist dafür verantwortlich, alle mit dem Bankgeschäft und Bankbetrieb gewöhnlich verbundenen Risiken in angemessener Weise zu begrenzen. Dazu gehört auch operationelles Risiko und daraus kann man dann die rechtliche Verantwortung für IT-Risiko mit konstruieren. Also das geht. Und dann kann eben die FMA sagen: "Gut, wir haben hier eine Richtlinie, da steht drin, was wir uns unter angemessen vorstellen", und damit geht das so. Aber es ist halt eine juristisch eher schwache Konstruktion und das sollte DORA dadurch beheben, dass man einerseits jetzt in DORA selber sogenannte Level 1 Rechtstext, also als EU-Verordnung wie ein Gesetz in allen Mitgliedsstaaten, richtig? Und dann die Level 2 Texte, das sind also die Mandate, Technical Standards und so weiter, die aufgrund von DORA durch die europäischen Bankaufsichtsbehörden erlassen werden dürfen - das wäre dann so etwas wie eine österreichische Verordnung durch eine Behörde - wollte man dadurch rechtlich bindende und dann auch noch in der ganzen EU einheitliche Regelungen haben. Aber wie gesagt, inhaltlich sind da sehr viele Dinge dabei, die jetzt für die Bankenaufsicht nicht neu sind und auch aus dem Thema IT-Risiko heraus nicht neu sind, sondern die auch aus internationalen Normen und Best Practices kommen.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Jonathan Denzel: Richtig. Also der Teil mit den Normen ja, aber noch nicht verpflichtend aus den EBA Guidelines, die noch nicht ganz in diesem Umfang aus dem, was ich bisher herausgelesen habe, mit drin sind.

Stefan Unteregger: Genau. DORA ist teilweise detaillierter, hat teilweise explizitere Ansprüche. Generell waren die EBA-Guidelines immer - also technologieneutral ist DORA auch, da steht ja auch nicht drinnen, es muss folgender Verschlüsselungsalgorithmus verwendet werden, weil das wird schneller veralten, als wir die gesetzlichen Grundlagen dazu erneuern können. Also technologieneutral, prinzipienorientiert ist DORA auch - die EBA-Guideline hatte halt noch einen Schritt allgemeiner formuliert und so weiter, während DORA jetzt eben aufgrund des expliziten gesetzlichen Auftrags, den DORA ja darstellt, dann auch in den Technical Standards, also in den darunter geordneten, für gewisse Sachen einfach klarere und bindende Vorgaben geben kann. Die EBA-Guideline und andere nationale Richtlinien waren eben juristisch nicht bindend, aber waren dadurch, dass sie ja eben Interpretationen der sehr allgemeinen Richtlinien waren, durchaus durchsetzbar. Also es ist jetzt auch nicht so, dass wir dann jahrelang den Banken hätten sagen müssen, es gefällt uns zwar nicht, was ihr da macht, aber wir können euch nicht zwingen. So nicht ganz richtig. Wobei man da auch sagen muss, dass wir die Banken direkt behördlich zu was zwingen, ist der ganz letzte Schritt in sehr vielen Fällen. Ja, also in den allermeisten Fällen funktioniert es ja so, die Aufsicht stellt Mängel fest. Mit der Bank wird das Beheben besprochen und die Bank setzt es dann um, ohne dass man, mit Androhung von Verwaltungsstrafen und weiß Gott was (...) dazu wirklich rechtlich bindend verpflichten muss.

Jonathan Denzel: Wie läuft die Eskalation weiter, wenn eine Bank sich beim ersten Mal noch nicht dran gehalten hat und bei der nächsten Prüfung kommt dasselbe wieder?

Stefan Unteregger: Nicht nach einem starren Muster ist einmal die ganz allgemeine Antwort. Ich bin da auch zugegebenermaßen einmal so ein bisschen an der falschen Seite. Ich bin praktisch der Verkehrspolizist mit der Radar-Pistole, der dann die Erkenntnisse weitergibt. Und diese ganzen Fragen, das ist für die Großbanken EZB (Enforcement & Sanctions heißt das dort) und nationale Ebene LSI, FMA behördliche Abteilung. Also das sind dann die sich um weitere Dinge kümmern. Aber generell, die Aufsicht hat sowohl auf europäischer als auch auf nationaler Ebene einen Strauß von Instrumenten, der dann immer unangenehmer werden kann. Und da sind dann auch im behördlichen Verfahren auf der nationalen Ebene wie auch auf der europäischen Ebene von Verwaltungsstrafen bis hin zu - auf der ganz, ganz letzten Ebene - Entzug der Konzession. Also das geht von ‘böse schauen’ bis ‘es gibt euch nicht mehr’ und dazwischen ist ein sehr weites Feld. Aber wie gesagt, es gibt jetzt auch keine Automatismen in dem Sinne, dass man sagt: verbindliche Regel, beim dritten Mal wird die Bank zugesperrt.

Jonathan Denzel: Danke. Die nächste Frage ist: Wie würden Sie die Komplexität der DORA einordnen zu dem, was es bisher gab, nachdem die DORA ja nicht nur der

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

primäre Gesetzestext ist, sondern auch jetzt der erste und zweite Batch an Richtlinien und technischen Standards herauskam. Wie würden Sie da die Komplexität einordnen?

Stefan Unteregger: Nicht viel höher als das, was wir schon machen. Geprüft haben wir bereits in einem vergleichbaren Detailgrad und Tiefegrade. Was sich ändert, ist vor allem die rechtliche Grundlage, die wir jetzt dafür haben. Aber schon vorher eben durch die EBA-Guideline, dadurch, dass man sich beim Prüfen an - in unserem Bereich - europäischen Prüfstandards orientiert, auf nationaler Ebene, nach unseren nationalen Prüfprogrammen, die auch da detaillierter sind, ist da nicht so viel Komplexität, die dazu kommt für das tatsächliche Prüfen. Es gibt ein paar Dinge, die in DORA jetzt dann eben wie gesagt expliziter gefordert werden, wo man in Zukunft also dann tatsächlich nach einem harten Kriterium abprüfen kann, ob eine Bank das tut. Da gibt es im Bereich Sicherheitstests zum Beispiel ein paar Dinge, dass kritische Applikationen alle sechs Monate getestet werden müssen. Das war bisher so explizit nicht forderbar. Aber geprüft haben wir schon in der Vergangenheit, ob jetzt grundsätzlich Pen-Tests, Sicherheitstests, Secure Code Reviews usw. durchgeführt werden. Das heißt, vom Prüfaufwand ist es effektiv genau dasselbe. Ich erhebe hier auch so wie früher: Was tut die Bank in dem Bereich? Nur beim Beurteilungsmaßstab habe ich dann in Zukunft mit DORA in ein paar Dingen wirklich klarere Kriterien, wo ich sagen kann: Okay, hier wird dagegen verstoßen. Wo ich bisher abwägen musste, ist es ausreichend, passt mir das in die EBA-Guideline rein? Aber wie gesagt, von der Komplexität des Prüfens her - der Detailgrad teilweise ein bisschen anders - aber die Prüffelder erweitern sich durch DORA nicht maßgeblich. Am ehesten noch im Bereich Outsourcing Risiko, wo noch dem DORA Begriff der 'Third Party Providers', der Begriff jetzt weiter gefasst ist, aber im Bereich IT-Risiko, Security Testing, Incident Management eigentlich nicht so sehr.

Jonathan Denzel: Das passt eigentlich sehr gut zur nächsten Frage. Wie bewerten Sie da die Verhältnismäßigkeit in der DORA, weil sie ja als Leitprinzip ganz oben groß mit angebracht ist? Dann gibt es eine kleine Ausnahme für diese Kleinstunternehmen und alles andere ist, wie Sie sagen, ein hartes Kriterium. Also wie läuft auch in dieser Prüfung vielleicht erst die Verhältnismäßigkeit ab? Was können Sie dazu sagen?

Stefan Unteregger: Verhältnismäßigkeit ist immer schon ein ganz wichtiges Thema. Also das hatten wir in unseren Prüfungen auch schon lange bevor DORA auch nur am Horizont aufgetaucht ist. Es ergibt sich eigentlich auch zwingend, dass hier in den Vorschriften, in den Guidelines und auch in den technischen Standards in DORA immer noch an vielen Stellen steht, in angemessener Weise oder adäquate Verschlüsselung oder dergleichen. DORA zieht natürlich gewisse Mindeststandards durch die Formulierung verbindlich ein. Aber Proportionalität ist ja eben auch dort, wie Sie gesagt haben, immer drin. Und durch diese grundsätzliche Technologieneutralität und Prinzipienorientierung ist die Ebene der Proportionalität immer drin. Und was da aber auch eine wichtige Message ist, die wir auch den Banken jetzt schon im Vorfeld mehrmals mitgegeben haben: Proportionalität heißt ja nicht zwingend, weil ich kleiner bin, muss ich mich um bestimmte Risiken nicht kümmern. Also es ist ja bei diesen ganzen Sachen in angemessener

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Weise und risikoadäquat und so weiter, auch ganz stark davon abzustellen, wie stark betrifft mich das? Also auch ein kleines Institut, mit aufgrund des Geschäftsmodells besonders hoher Abhängigkeit von IT - also, ein Online-Wertpapierbroker hat ganz andere Anforderungen an die Verfügbarkeit als - wenn wir jetzt im DORA Bereich bleiben - ein Versicherungsinstitut, das Lebensversicherungen anbietet und wo jetzt innerhalb von zwei Stunden irgendwie Tausend Transaktionen durchgeführt werden können oder so, vielleicht nicht so im Vordergrund steht. Wobei ich jetzt für die Versicherungsaufsicht nicht sprechen möchte. Also nur als grundsätzliches Beispiel. Oder eine Bausparkasse, hat eine wesentlich größere Toleranz zu: Die Systeme gehen jetzt einmal eine Stunde nicht. Weil in der Stunde wollen ein paar Leute einen Bausparvertrag eröffnen, ein paar Leute wollen ein Bauspardarlehen haben und wenn nicht gerade Jahresende ist, werden nicht einmal Kontoauszüge gedruckt. Beim Online-Broker, wie gesagt, schaut das ganz anders aus. Wenn dort eine Stunde die Systeme stehen, ist es ja ganz anders. Und daher, auch wenn jetzt die fiktive Versicherung Bausparkasse riesengroß ist und Millionen Kunden hat und der Online-Broker vielleicht viel weniger, hat der viel höhere Notwendigkeit, sich um die IT-Risiken zu kümmern. Also das muss man auch immer hier mit bedenken. Das heißt jetzt nicht: Ich bin ein kleines Institut, ich brauche keine Berechtigungsverwaltung.

Jonathan Denzel: Ja, ich habe mir als Beispiel rausgenommen: IKT Drittanbieter-Audits. Was etwas ist, dass ich bisher aus den EBA-Guidelines noch nicht herausgelesen habe. Dass man wirklich auch Audits durchführen muss. Und in der DORA scheint mir das so, als ob das als hartes Kriterium mit drin ist, dass man sich einen Plan machen muss, wie man seine IKT Drittanbieter, auditiert.

Stefan Unteregger: Das ist tatsächlich etwas, wo DORA tatsächlich klarer formuliert, dass das erwartet wird. Wo wir aber bisher schon - hier halt nicht in der EBA Guideline zu ICT-Risk, sondern in der EBA Outsourcing-Guideline - auch schon die Verpflichtung haben, diese Prüf- und Einschaurechte vertraglich vorzusehen. Und das ging immer schon mit der Erwartung einher, dass man die bei Bedarf auch ausübt. Also, auch hier ist der Unterschied gar nicht so groß. Und auch hier hat man natürlich sowohl in der Vergangenheit unterschiedliche Anforderungen gestellt an ein kleines Finanzinstitut mit einem riesigen IT-Dienstleister, wo man jetzt nicht erwarten wird, dass der den riesigen IT-Dienstleister jedes Jahr nach Strich und Faden auditiert, als an irgendeine große international agierende Großbank, die ganz anders vorgehen kann. Und das wird auch mit DORA sicherlich noch ein Thema sein. DORA gibt ja gerade in dem Bereich dann auch Möglichkeiten für Joint Audits, also dass nicht jeder einzelne Kunde dann mit seiner eigenen, möglicherweise winzigen, Innenrevisionen da sich ich das Ganze gibt. Es gibt die Möglichkeit sich auf Audits von Externen zu stützen teilweise.

Jonathan Denzel: Bedeutet das, die Wirtschaftsprüfer werden in Zukunft Audit Berichte für die IT-Anbieter durchführen? Auf die kann man sich stützen?

Stefan Unteregger: Ich könnte mir vorstellen, dass die Wirtschaftsprüfer das anbieten. Ich bin mir jetzt auch nicht sicher, was die so tun werden. Eine wichtige Botschaft, die

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

wir in dem Zusammenhang auch schon vor DORA den Banken immer wieder mitgegeben haben, weil auch immer wieder schon in der Vergangenheit die Frage aufkam, von wegen Zertifikate, ISO Zertifizierungen oder so, ob das denn ausreicht? Da war unsere Aussage immer schon - das wird mit DORA jetzt auch nicht anders - solche Zertifikate sind nützlich, aber sie sind kein Allheilmittel. Also nur, weil jetzt irgendwo der Stempel darauf ist: Zertifiziert, heißt das nicht - sowohl für uns als auch für jemanden, der sich da beim Drittanbieter verlassen will - 'Dort ist ohnehin alles zertifiziert und kann nichts mehr passieren. '

Jonathan Denzel: In dieser Welt leben wir nicht.

Stefan Unteregger: Genau. Es gibt erstens mögliche Einschränkungen bei den Zertifikaten, dass schon mal das grob gar nicht alles abdeckt, was man aber erst genauer erkennt, wenn man den Detailbericht liest. Oben der große Stempel, schaut sehr hübsch aus. Es gibt bei den externen Prüfern auch immer wieder mehr oder weniger genaue Überprüfungen. Also nur, weil irgendwo am Papier gewisse Voraussetzungen erfüllt sind. Natürlich ist es grundsätzlich besser, als wenn man überhaupt keine Indikation hat, ob sich der Drittanbieter an irgendwelche Standards zu halten versucht. Und wir haben auch den Banken immer gesagt, wir geben euch jetzt zwar nicht vor 'ihr braucht eine ISO 27000 Zertifizierung' aber wenn ihr eure IT-Sicherheit an der ISO 27000 ausrichtet oder an einem anderen vergleichbaren internationalen Standard - also wir sind da auch standardneutral - dann ist es wahrscheinlich nützlicher, als euch von null weg zu überlegen, was könnte man denn im IT-Sicherheitsbereich so alles tun? Aber stehen und fallen tut es immer mit der tatsächlichen Anwendung, mit Risiko angemessenen Prozessen und Maßnahmen und Kontrollen. Und das ist der Punkt, um den man halt nicht herumkommt.

Jonathan Denzel: Bedeutet im Prinzip für kleine Bankhäuser ist die Erwartung, dass sowas auch anlassbezogen auditiert werden - dass sowas eine Möglichkeit sein könnte zu sagen, für uns ist das Prüfintervalls anlassbezogen, wenn wir sagen, es gab einen Vorfall.

Stefan Unteregger: Ich gehe davon aus, dass es darauf hinauslaufen wird, muss aber hier dazu sagen, dass ich für die Erwartungen gegenüber kleinen Bankhäusern gar nicht sprechen kann, wenn wir hier in der Hauptabteilung für die Großbankenaufsicht sind. Also das wären die Kollegen ein Stock höher. Aber von der grundsätzlichen Richtung her wird das nicht so falsch sein.

Jonathan Denzel: Okay, dann das Nächste ist: Wissen Sie heute schon, wie die Prüfung der Banken zu DORA aufgebaut sein werden? Werden stichprobenartig Banken ausgewählt? Wird dann innerhalb der Banken stichprobenartig Themengebiete ausgewählt oder sind das Vollprüfungen von allem? Wie kann ich mir das vorstellen?

Stefan Unteregger: Hier gilt generell, dass sich da durch DORA auch nicht allzu viel ändert. Wie gesagt, wir machen schon seit mehreren Jahren Prüfungen im Bereich IT-Risiko und wir werden auch in Zukunft sicherlich nicht weniger Prüfungen im Bereich

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

IT-Risiko machen. Das heißt, nur weil wir jetzt hier eine neue Rechtsgrundlage dafür haben, ändert sich hier auch der Ansatz der Prüfplanung nicht. Was passieren kann, ist, dass bestimmte Schwerpunkte - das ist auch jetzt DORA unabhängig - Also was immer wieder regelmäßig passiert ist und laufend passiert ist, dass gewisse Schwerpunktthemen für ein bestimmtes Jahr gesetzt werden. FMA und OeNB veröffentlichen auch einmal im Jahr - da gibt es dann immer Presseaussendung - Schwerpunktthemen der Aufsicht. Und Prüfungen und andere Aufsichts-Aktivitäten werden dann unter anderem nach diesen Schwerpunktthemen ausgerichtet. Heißt dann auch nicht, dass in dem Jahr nichts anderes geprüft werden kann und darf, heißt aber, dass das die Bereiche sind, die uns besonders interessieren. Wenn jetzt so was Neues, so eine neue Grundlage wie DORA dazukommt, wird es sich voraussichtlich anbieten, dass man sagt: Gewisse Themen von DORA wären gut geeignete Schwerpunktthemen. Schwerpunktthemen, gerade jetzt laufendes Jahr und die letzten Jahre, da war IT-Sicherheit, Cybersecurity und auch IT-Outsourcing, waren da auch schon drin. Also das ist jetzt nicht so, dass man sagt, DORA und jetzt erstmals Schwerpunkt IT-Sicherheit. Das heißt, da hat DORA jetzt weniger Einfluss auf die Prüfthemen, als man vielleicht meinen möchte. Weil eben die Themen an sich, die auch in DORA behandelt werden, bisher auch schon in der Planung drin waren.

Jonathan Denzel: Ich habe den Teil noch nicht ganz verstanden. Suchen Sie sich einzelne Banken stichprobenartig raus?

Stefan Unteregger: Generell funktioniert die Prüfplanung so - also jetzt Großbankenbereich gesprochen. Das sind ja nicht so viele in Österreich. Zahl schwankt zwischen sechs und acht, also unter zehn. Das heißt, die Großbanken werden ohnehin regelmäßig geprüft. Das heißt, bei denen geht es nicht so sehr darum, wird hier eine Bank stichprobenartig ausgesucht. Sondern da geht es darum, die Großbanken sind seitens EZB und national in der Aufsicht, wir arbeiten da ja ganz, ganz stark mit. Jede Großbank hat ein Joint Supervisory Team, wurde von der EZB gegründet, wird auch von Kräften aus der nationalen Aufsicht gestaffed. Also da sind aus OeNB und FMA Leute drin. Dieses JST hat diese spezielle Großbank die ganze Zeit über im Blick, betrachtet dort die Risiken. Und die JST überlegen sich welche thematischen Prüfungen sie dann jeweils fürs nächste Jahr - weil die Prüfplanung geht ja im Vorfeld los - haben wollen. Das heißt, da ist also nicht die Frage, kommt die Großbank X nächstes Jahr überhaupt dran, sondern die Frage ist, welches Thema prüfen wir dort? Und da sind eben auch die Themen, die jetzt dann mit DORA kommen, auch jetzt schon immer wieder drin. Im LSI [Anmerkung: "Less Significant Institutions"]-Bereich, wo wir viel mehr Banken haben und auch ganz unterschiedliche Größen, sind wir eher in dem Bereich, wo gewisse Banken, wenn Sie so wollen, stichprobenartig ausgewählt werden. Gewisse Banken aufgrund ihrer Größe, ihrer Wichtigkeit häufiger und tourlicher, also da ist das ein mehrstufiges Planungsfeld - Auch wieder hier aber nicht meine Ecke, also kann ich Ihnen nicht so genau sagen. Aber grundsätzlich funktioniert es dort eher so. Und die Themen, die geprüft werden, das gilt jetzt eben sowohl auf europäischer als auf nationaler Ebene, die werden in der nationalen Prüfplanung eben je nach strategischen Schwerpunkten, besonderen Interessen,

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Anlassfällen und so weiter jeweils geprüft. Auch das ändert sich durch DORA jetzt natürlich.

Jonathan Denzel: Dann habe ich noch zwei detailorientierte Fragen. Das eine ist, was Toleranzen angeht für Verspätungen. Weil es ja doch so ein paar Maßnahmen gibt, die für viele Banken überraschend kommen, vor allem für kleinere Banken, die es noch nicht so ganz auf dem Schirm haben. Gibt es da Toleranzen, wo man sagt, wenn es im ersten halben Jahr noch nicht da ist, dann prüfen wir das im zweiten halben Jahr. Oder ist es von Tag eins, dass die Erwartungshaltung ganz klar ist und ab heute gilt es?

Stefan Unteregger: Also DORA und die darunterliegenden Technical Standards sind mit dem 17. Januar 2025 anwendbar und in Kraft. Das heißt, ab diesem Zeitpunkt gelten die für uns und für die Banken und sind Prüfmaßstab und dergleichen. Aber es ist ja ohnehin nicht so, dass wir im Jänner 2025 alle österreichischen Banken durch prüfen können. Also effektiv (...) auch hier wieder behördliche Erwartungshaltung und so weiter, eher FMA und so. Aber in der Praxis schon jetzt sind einige von den Themen, die mit DORA verbindlich sind, bei uns durchaus im Schwerpunkt. Wir stellen regelmäßig fest, dass es da Mängel gibt und es gibt dann regelmäßig Fristen zur Behebung. Das wird mit DORA auch wieder nicht sehr viel anders sein. Also auch hier gilt, wenn Mängel festgestellt werden, hat die Bank das zu beheben. Die laufende Aufsicht überwacht das, kann da eben auch Fristen setzen, kann den Fortschritt überwachen.

Jonathan Denzel: Kann sehr hohe Strafzahlungen festlegen?

Stefan Unteregger: Könnte auch sehr hohe Strafzahlungen festlegen. Aber wie gesagt, das ist dann die Ecke, wo ich Ihnen auch nicht sagen kann, wie das konkret da gehandhabt wird. Was ich Ihnen sagen kann, ist gerade im Bereich IT-Risiko, dass wir dort prinzipiell schon - und auch das wird mit DORA nicht anders - häufig die Situation haben, dass gerade größere Mängel garnicht schnell behebbar sind. Wenn wir bei einer Bank feststellen, dass dort der ganze Bereich Asset Management, Konfiguration Management Datenbank noch im Aufbau befindlich ist, Datenqualität schlecht, CMDB unvollständig, Asset Classification dort noch nicht drinnen. Das ist nicht in drei Monaten zu beheben. Das ist dann ohnehin was, wo in der Behebung mit entsprechendem realistischen Zugang gearbeitet werden muss. Da hilft es auch nichts, wenn dann die Behörde sagt in zwei Monaten funktioniert das auch, weil das funktioniert in zwei Monaten nicht. Und auch das ist jetzt mit DORA nicht anders. Es sind ja eben keine komplett neuen Anforderungen. Das wäre jetzt was anderes bei den Basler Eigenmittelbestimmungen damals. Die, von null auf jetzt, hatten die Banken, Eigenmittel zu bestimmen nach dem und gewisse Dinge zu melden und weiß der Gott was. Wenn das eine Bank dann nicht getan hat, war dann sofort. Die Anforderungen an das IT-Risikomanagement, wie gesagt, die sind ja schon in der Vergangenheit da gewesen. Und da hat es auch in der Vergangenheit schon Mängel gegeben. Und jetzt kommen sie mit DORA auf einer rechtlich verbindlichereren Ebene und es wird auch da wieder Mängel geben. Also wie gesagt, auch hier erwarte ich jetzt nicht, dass es da irgendwie einen Stichtag bezogenen Prüflauf, durch alle Banken

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Österreichs geben wird. Auch weil das logistisch gar nicht möglich wäre. Sondern, dass hier das, was wir laufend tun, dann eben auf der neuen Grundlage und mit den diversen Konkretisierungen und möglichen Verschärfungen geprüft wird. Auch wenn eine Bank, was in der Praxis nicht oft passiert, aber wenn die jetzt sagen würden: Oh, wir teilen die Meinung und die Aufsicht hier nicht, dass wir das tun müssten, hätte man in der Vergangenheit natürlich wesentlich besser streiten können von wegen 'was muss man überhaupt tun'. Während bei Dingen, die in der DORA explizit drinnen stehen, der Schritt wegfallen würde. Aber das ist tatsächlich auch etwas, was nicht wahnsinnig oft vorkommt, weil wir uns ja jetzt auch nicht extra neue Anforderungen für die Banken ausgedacht haben in dem Bereich, sondern die bisherigen Ansprüche sich an internationale Standards wie auch eben der ISO 27000 und dergleichen, COBIT usw. orientiert haben. Also das jetzt nichts ist, wo wir sagen, Kraft unser Aufsicht müsst ihr alle Dokumentationen in blauen A4 Ordnern abheften. Sondern der Anspruch ist: eigenentwickelte Software ist zu testen und zu dokumentieren. Auch wenn im BWG nirgends Testen oder Dokumentieren drinsteht, aus der Interpretation. Bitte versuche den Standpunkt zu vertreten, dass es nicht angemessen ist, Software zu testen oder zu dokumentieren [Leicht ironisch]. Funktioniert nicht so gut. Aber wie gesagt, wenn jetzt in der DORA dann explizit drinsteht, für Systeme, die kritische Funktionen unterstützen, sind Sicherheitstests alle sechs Monate durchzuführen. Dann brauche ich mit der Bank nicht diskutieren, ob sechs Monate angemessen sind oder nicht. Tatsächlich, wie gesagt, hatten wir aber die Situation auch nicht oft, dass man jetzt überhaupt groß diese Diskussion führen muss. Ist das überhaupt verbindlich oder nicht?

Jonathan Denzel: In der DORA werden viele Aufgaben von einem SOC, einem Security Operations Center, gefordert. Aber es wird nicht explizit erwähnt, dass ein SOC einzuführen ist. Gleichzeitig gibt es aber die Threat Intelligence und natürlich das Incident Management und alles, was dann noch dazu gehört, die Fähigkeit, Assets fast instantan zu isolieren etc. Ist es in der Praxis im Prinzip eine Verpflichtung zu einem SOC?

Stefan Unteregger: Das ist so ein Bereich, wo Proportionalität relativ stark mit ins Spiel kommt. Also ohne jetzt hier klar ja oder nein zu sagen, vor allem auch wieder, weil sich die Frage besonders bei den kleineren Banken stellen wird. Das ist genau so ein Fall, wo man im Lichte der Proportionalität halt abwägen muss, was kann man angemessener Weise fordern? Was da allerdings schon auch dazu kommt, dass ja relativ viele kleinere Finanzinstitute gemeinsame IT-Dienstleister haben. Also, dass hier dann schon mehr passieren kann, als 'man braucht das von jedem einzelnen Bank- oder Wertpapier-Dienstleister. Aber gerade diese Dinge, SOC, welche Aufgaben da drinnen ist, rund-um-die-Uhr-Verfügbarkeit, in welchem Ausmaß, weil da gibt es ja auch Abstufungen von 'da sitzen ständig zehn Leute im Schichtdienst' oder 'es gibt halt immer zwei, die auf Rufbereitschaft sind'. Das sind genau diese Punkte, wo dann Proportionalität reinkommt. Wenn eine große international tätige Bank sagt 'während der normalen Geschäftszeiten sind zwei Leute da und am Wochenende vielleicht einer auf Rufbereitschaft' wird das möglicherweise nicht so angemessen sein. Und auf der anderen Seite wird man von einer

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

kleinen Bank mit 100 Mitarbeitern auch nicht sagen, warum sind da nicht zehn Leute 24/7 im Schichtdienst? Weil die müssten dann 30% ihrer Belegschaft im SOC drinnen haben, wenn sie drei Schichten brauchen. Das sind genau diese Themen, wo gerade auch mit DORA Proportionalität ein ganz wichtiger Faktor ist.

Jonathan Denzel: Okay, sehr gut. Abschließend noch die Frage: Wie haben Sie DORA aufgenommen? Was waren Ihre Erwartungen an dieses Gesetz? Und was hat Sie vielleicht überrascht?

Stefan Unteregger: Überrascht hat mich ehrlich gesagt nicht wahnsinnig viel, weil wir die ganze Zeit über in den Prozess eingebunden waren. Also ich bin selber seit 2015 in der EBA Taskforce on IT-Risk. Also ich habe die ICT Guidelines mitgeschrieben, die kommen aus der Taskforce. Die ersten Vorarbeiten zu DORA, der diverse Werdegang, die Beobachtung und die nationalen Stellungnahmen, da waren wir überall involviert. Also überrascht kann man jetzt so wirklich nicht sagen. Es gab im Vorfeld von DORA ein paar Dinge, die wir uns vielleicht ein bisschen anders gewünscht hätten. Beispielsweise ist das Mandat für den Technical Standard on ICT Riskmanagement (...) enthält gewisse Themen nicht, die in der EBA-Guideline drinnen sind.

Jonathan Denzel: Zum Beispiel?

Stefan Unteregger: Zu den 3 Lines of Defense, die in DORA schon im Level 1, also in der DORA selber genannt sind, hat der RTS kein spezielles Mandat. Projektmanagement, Softwareentwicklung ist, soweit ich mich erinnern kann, nicht explizit genannt und ist aber in der EBA Guideline drin. Da hätten nicht nur Österreich, sondern viele Länder auch im Vorfeld gehofft, dass da ein bisschen mehr Kongruenz passiert, damit man mit DORA und mit dem Technical Standard dann alle Themen geregelt hat. Ist so nicht gekommen, aus verschiedenen Gründen.

Jonathan Denzel: Also die drei Lines of Defence im Projektmanagement?

Stefan Unteregger: Nein, die drei Lines of Defence im IT Risikomanagement. Die sind mit DORA auch gefordert. Das ist ein ganz wichtiger Punkt. Die Sache ist, dass sie im Regulatory Technical Standard on ICT-Risk Management werden keine sehr konkreten Anforderungen dazu drinstehen können, weil die im Mandat nicht explizit drinnen sind, während in der EBA Guideline dazu schon mehr drin war. Und die Botschaft ist aber keineswegs jetzt, mit DORA muss man sich das nicht mehr kümmern, weil es da nicht drinsteht. Im Gegenteil, es steht ja in DORA, die drei Lines of Defence und das ICT Risikomanagement ist ja im Level 1 Text schon genannt. Das ist das eine. Und die EBA Guideline wird ja auch weiter bestehen nach DORA. Die wird zwar voraussichtlich angepasst werden, damit sie mit DORA dann gut zusammenpasst, im Laufe der nächsten ein, zwei Jahre irgendwann. Aber die bleibt ja auch. Also das war zum Beispiel was, wo wir im Vorfeld gehofft hätten, dass gewisse Sachen da auch mehr Berücksichtigung finden. Aber wie gesagt, so jetzt überraschend war nicht

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

wahnsinnig viel. Es hat sich im parlamentarischen Prozess, im Trilog und so, also in dem ganzen europäischen Gesetzgebungsverfahren haben sich immer wieder Dinge geändert. Nationale Delegationsrechte sind teilweise noch einmal komplett umformuliert worden und so, also da gab es schon ein paar Dinge. Aber wie gesagt, wir sind in diese ganzen Prozesse sehr eingebunden. Und auch jetzt bezüglich der Umsetzung von DORA und Ausarbeitung der Regulatory Technical Standards das läuft in einer gemeinsamen Aktion der Europäischen Finanzaufsichtsbehörden - also EBA, ESMA und EIOPA - und aller zuständigen Aufsichtsbehörden europaweit wird koordiniert über ein Subkomitee des gemeinsamen Ausschusses der europäischen Finanzaufsichten, also der europäischen Finanzaufsichten. Wenn sich die EBA's koordinieren, tun sie das im gemeinsamen Ausschuss, im Joint-Komitee. Wenn das Joint-Komitee irgendwas tatsächlich umgesetzt - weil das Joint-Komitee ist die Koordination auf oberster Ebene - wenn die was umgesetzt wollen für den gesamten Finanzsektor, gibt es ein Subkomitee. Und dieses 'Joint Komitee Subkomitee on Digital Operational Resilienz', das Gremium, das jetzt seit über einem Jahr die Ausarbeitung der ganzen Technical Standards koordiniert, das wird auch von den ganzen Ländern beschickt. Also da bin ich zum Beispiel der OeNB Vertreter drinnen und die koordinieren die Arbeitsgruppen, die die Technical Standards schreiben. Also da haben wir auch wir hier im Team Leute sitzen und von der FMA sind Leute in den Arbeitsgruppen, die diese Technical Standards mit verfassen und die dann inhaltlich, also überraschend kann uns da nichts. Im Gegenteil, das kommt von uns. Und das Ganze geht dann ja auch noch durch alle Gremien und Instanzen durch. Also das wird inhaltlich auf der Ebene abgestimmt, geht dann ins Joint-Komitee, wo es vom Top-Management der jeweiligen Vertreter dort beschlossen wird, geht dann in die Boards of Supervisor der ESAs, wo es dort final beschlossen wird und wird von dort an die Europäische Kommission weitergegeben, damit die das dann noch juristisch prüfen und im Amtsblatt kund machen. Aber wie gesagt, in dem Prozess sind wir ja maßgeblich eingebunden.

[Kurze Unterbrechung der Aufnahme]

Also, das ist eben, zum Beispiel, vom Ablauf her. Also diese Dinge haben wir teilweise mitgeschrieben. Jetzt beim Second Batch ja doch auch, weil da ist Threat Led Penetration Testing dabei. Österreich setzt ja gerade in Vorbereitung dazu TIBER um.

Jonathan Denzel: Genau, angelehnt an TIBER.

Stefan Unteregger: Genau. Das haben wir ja auch angeleiert, als DORA am Horizont aufgetaucht ist und wir gesagt haben: Okay, da werden wir dann für nationales Threat led Penetration Testing was brauchen, dann wurde das hier umgesetzt und die Kollegen, das ist paar Stockwerke tiefer, das TIBER-Cyber-Team, die Kollegen, die das umsetzen, sind in Abstimmung mit der Arbeitsgruppe, wo unter anderem auch der RTS on Penetration-Testing erarbeitet wird. Und die Arbeitsgruppe, da konkret die zu TLPT, die wird von der Bundesbank auch ganz stark mit beeinflusst, wo die Leiterin des dortigen TIBER Cyber Teams dort dann auch in der Arbeitsgruppe drinnen sitzt. Und die kommen jetzt eben in die Konsultation. Aber eben in den Arbeitsgruppen werden die Texte formuliert.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Dann gehen die Texte ins Joint-Komitee-Sub-Komitee. Als OeNB Vertreter koordiniere ich da dann noch einmal, dass die OeNB-Position da in die Kommentare einfließt, genauso FMA-seitig und FMA und OeNB stimmen sich da gegenseitig ab. Dann kommen diese, wenn es da inhaltliche Einwände gibt oder (...) bringen wir als nationale Vertreter das in das Sub-Komitee. Die dortigen Workstream-Leiter bringen das dann wieder in die Arbeitsgruppe und dann werden die Kommentare umgesetzt oder auch nicht. Dann gibt es irgendwann einmal einen finalen Text zum Abnicken im Joint-Komitee Sub-Komitee. Wenn wir sagen 'passt so weit' dann geht's eins weiter ins Joint-Komitee. Da könnte ich dann beim Briefing dem österreichischen Vertreter theoretisch sagen, hier erhebliche Einwände, bringt das zu Fall. Den Fall haben wir normalerweise natürlich nicht, weil das eben vorher schon im Sub-Komitee so weit Konsens erreicht wird. Und dann geht es eben ins Board of Supervisors - für unseren Bereich für die EBA - aber eben bei DORA in alle drei gleichzeitig. Und auch da sitzen ja wieder FMA-Vertreter, OeNB-Vertreter drin und können da zustimmen oder ablehnen. Wobei, wenn es einmal im Board of Supervisors ist, ist es recht spät. Dann müsste man- Das wäre ein ziemlicher Eskalationsschritt, wenn man sagen würde: Ich verweigere da die Zustimmung bei der Abstimmung. Aber wie gesagt, dafür gibt es ja vorher mehrere verschiedene Ebenen. Aber das ist alles- da sind jeweils auch die Länder auf diese Weise eingebunden. Und das ist etwas, was uns jetzt das ganze letzte Jahr schon massiv beschäftigt auch. Da wird eben die nationale Position konsolidiert oder in einigen Bereichen gibt es auch gar keine spezielle-. Da gibt es einen Entwurf aus dem Drafting Team. Ich schicke das bei uns im Haus herum. Damit hat jeder Bereich bei uns die Informationen und kann sich das mit seiner Perspektive durchschauen. Und wenn irgendwas drin ist, das über mich dann in die Arbeitsgruppe einbringen oder halt eben wie gesagt genauso FMA. Und auch die Abstimmung zwischen FMA und OeNB funktioniert da eigentlich auch reibungslos, kann man sagen. Und dann wie gesagt ist es damit eine österreichische Position. Und für diese ganzen höherstufigen Gremien, wo üblicherweise dann auch FMA und OeNB Vertreter gleichzeitig gebrieft werden, ist es dann auch nicht so, die FMA sagt dann ihrem Vorstand irgendwas anderes als wir. Vorher wird die österreichische Position zwischen FMA und OeNB abgestimmt. Die jeweiligen Vertreter könnten sich dann natürlich immer noch unterschiedlich verhalten, aber an sich ist somit gewährleistet, dass da alle Bereiche involviert sind. Jetzt für DORA natürlich noch ein bisschen spannender, weil es nicht nur die Bankenaufsicht betrifft, sondern eben FMA-seitig alle von deren Aufsichtsbereichen. Aber funktioniert auch. Wir stimmen uns inhaltlich mit der Bankenaufsicht ab. Die Bankenaufsicht stimmt sich FMA intern mit den anderen Aufsichtsbereichen ab. Und wenn jetzt die Versicherungsaufsicht für irgendeinen Punkt in einem RTS einen Versicherung-spezifischen Punkt rein reklamieren will, halten wir uns OeNB-seitig raus oder stimmen gegebenenfalls ab, ob der Bankaufsichtsbereich eine andere Position vertritt. Also das wird da markiert, als Position der Versicherungsaufsicht und geht so. Also das funktioniert in Österreich recht gut. Teilweise in anderen Ländern durchaus noch deutlich komplizierter, weil die Länder zum Beispiel, wo die Zentralbank bestimmte Funktionen hat, dann gibt es eine Bankaufsichtsbehörde, eine davon unabhängige Versicherungsaufsichtsbehörde und dann hat vielleicht irgendwie noch die Börse dort bestimmte Funktionen im Bereich

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Wertpapieraufsicht. Dann müssen die sich alle untereinander koordinieren und das dann vielleicht auch in größeren Ländern, wo das in jedem einzelnen dieser Häuser noch viel mehr Leute sind. Die FMA ist dort drüben. Die sind da und für IT-Risikothemen sind dort drüben ungefähr zehn Leute thematisch zuständig und bei uns im Haus ungefähr zehn Leute thematisch zuständig.

Jonathan Denzel: Die das auch prüfen?

Stefan Unteregger: Nein, die sich insgesamt mit IT-Risiko beschäftigen. Fürs Prüfen ist das jetzt wieder ein bisschen anders. Unter anderem, weil wir durchaus auch Prüfungen haben, wo wir nicht nur IT-Prüfer dabei haben. Also wenn ich jetzt eine Hausnummer nennen würde, wie viel IT-Prüfung, dann wäre das ein falscher Eindruck, weil es durchaus IT-Prüfungen gibt, wo dann Prüfer aus der Governance oder aus dem Outsourcing Bereich dabei sind.

Jonathan Denzel: Wie viele DORA Prüfer gibt es denn?

Stefan Unteregger: Na ja, DORA Prüfer in dem Sinn gibt es gar keine. Wir haben hier ein Team von IT-Prüfern im Großbanken Bereich. Es gibt ein Team von Prüfern für IT-Risiko im LSI Bereich. Es sind die Grenzen auch grundsätzlich bei uns nicht stark gezogen. Also es ist jetzt nicht so, dass es da eine Gruppe für IT-Prüfern gibt, die nichts anderes tun darf, sondern je nachdem. Eigentlich ist es in beiden Prüfabteilungen LSI und SI immer schon so gewesen, dass das ein großer Prüfer Pool ist, der halt in Gruppen organisiert ist. Und je nach den für die Prüfung notwendigen Skills werden die Prüfteams zusammengesetzt. Deshalb gibt es eben auch zum Beispiel Kreditrisiko-Prüfungen, wo ein, zwei IT-Experten mitkommen, sich bezüglich Datenqualität oder technische Umsetzung Rating Modell dort einzubringen und so weiter. Aber wie gesagt, es gibt spezialisierte IT Prüfer, und die führen in Zukunft Prüfungen auf Grundlage von DORA durch, und so wie wir bisher auf Grundlage der EBA Guideline oder ganz früher mal überhaupt auf Grundlage von: Gefällt mir nicht und im Paragraf 39 steht aber drinnen ihr müsst alles richtig machen. Das war natürlich damals eine Zeit, wo die Feststellungen viel grobkörniger sein mussten. Weil da hätte ich mir schwer getan zu sagen, 'ich will hier aber alle sechs Monate einen Sicherheitstest sehen', wenn nur irgendwo im BWG steht, 'die Risiken in angemessener Weise zu begrenzen'. Da wird es schwierig. Nun muss man auch sagen vor 10, 15 Jahren waren wir eher in dem Bereich (...) wenn ich dort so Fragen gestellt habe, wo die gegangen sind "Ja, Sicherheitstests, da planen wir ab nächstes Jahr ein erstes Pilotprojekt" und dann konnte man feststellen, bisher gibt es noch keine Sicherheitstests oder Pen Tests, maximal einer pro Jahr für irgendein Ding und das ist jedenfalls nicht genug. Also da waren auch die Finanzinstitute noch deutlich nicht so weit. Und insofern haben sich da die beiden Dinge ganz gut aufeinander zu entwickelt. Und jetzt aber schon seit einigen Jahren sind durch die EBA-Guideline bzw. auch schon im Vorfeld, EBA-Guideline, weil die Banken ja auch bemerkt haben, da kommt jetzt mehr, haben die schon wesentlich mehr aufgebaut. Wir haben da die Ressourcen und das Know-how aufgebaut und so entwickelt sich das eigentlich schrittweise weiter. Und

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

DORA ist da jetzt nicht so der riesige Sprung im Umfang. Was durch DORA eher dazu kommt, komplett neu, sind Dinge, die jetzt so die laufende Prüfung gar nicht so sehr betreffen. Das Incident Reporting, also die Meldeverpflichtung für IT bezogene Vorfälle, wird deutlich erweitert. Da gab es ja bisher in Österreich nur die PSD 2, also ZADIG (...) also die Umsetzung von der PSD 2 für das ganze Incident Reporting von den Zahlungsdiensten. Das wird ja mit DORA deutlich erweitert für die sicherheitsrelevanten Vorfälle, und alle Finanzdienstleister, nicht nur Banken. Das ist eine Sache. Das ist jetzt aber für uns in der Prüfung wieder relativ egal. Also wir hatten bisher schon Prüfhandlungen zum Incident Management und ob man dort jetzt auch schaut, ob die Bank-, wenn wir dort eh schon Incidents prüfen und schauen, wie hat die Bank das gehandhabt und gibt es einen Lessons Learned Prozess und wie ist die Eskalation passiert? Kommunikation nach außen und so weiter. Ob man dann am Ende noch schaut: Okay, erfüllt der Fall die DORA Kriterien? - Ja, die Bank hätte ihn melden müssen. Hat sie ihn gemeldet?

Das ist ein Prüfschrittchen mehr, aber jetzt nichts wo ich sage: Ach um Gottes willen, mit DORA ist da jetzt alles anders. Und in den RTS und in DORA zum Incident Handling stehen halt auch wieder Dinge drin, wo man jetzt der Bank sagen kann: Ja, aber es ist dann Eskalation und so weiter vorgesehen (...). Also das ist die-, es sind erhöhte Meldeverpflichtungen drinnen. Es gibt in Zukunft dann dieses verpflichtende Threat led Penetration Testing für die ganz großen.

Jonathan Denzel: Für ihre Banken?

Stefan Unteregger: Effektiv für unsere Banken. Da bin ich mir jetzt nicht ganz sicher, wie die offiziell kommunizierte Linie schon ist.

Jonathan Denzel: Die ist jetzt auch in dem Second Batch mit drin.

Stefan Unteregger: Ja, also der TLPT RTS, der ist jetzt da drinnen. Aber jetzt für die österreichische TIBER Umsetzung weiß ich nicht, ob die Kollegen schon offiziell was gesagt haben, welche Teilnehmer da aus DORA Sicht angepeilt werden sollen. Aber es ist sicher nicht ganz falsch, wenn man sagt, es wird vor allem oder nur oder so die significant institutions betreffen in erster Linie. Da haben wir aber eben vor über zwei Jahren schon angefangen haben, mit den TIBER-Vorbereitungen, um das jetzt zu haben, wenn dann DORA kommt. Und sehen auch, dass wir dadurch in einer besseren Position sind als ein paar andere Länder, die dort zu dem Thema national noch genau nichts haben und sich jetzt mit der EZB gemeinsam überlegen, wie sie da überhaupt tun, wollen. Andere Länder hatten das ja schon länger. Also Österreich ist da ja nicht wahnsinniger Vorreiter oder so, aber es ist gelungen, das rechtzeitig so einzufädeln, dass wir es jetzt haben. Das war ein großer Unterschied. Aber auch hier wieder in der Prüfung, egal. Wenn ich mir anschaue, wie eine Bank mit erkannten Schwachstellen umgeht, was ich auch schon auf der EBA Guideline getan habe, kann ich in Zukunft, wenn das eine Bank war, die einen TIBER Test hatte, kann ich sagen: Okay, ich hätte gern den Red Team Report. Was

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

steht da drin? Wie ist jetzt euer Maßnahmenplan? Gab es ein Purple Team Meeting, wo Red und Blue sich zusammen... Also da kann ich jetzt mehr Dinge machen.

Jonathan Denzel: Und was sie auch noch haben, ist der IKT Risikomanagement-Rahmen Bericht davon, den die Finanzinstitute anfertigen müssen, wenn ich das richtig verstanden habe?

Stefan Unteregger: Ja, aber auch da gilt: IT-Risiko mussten sie bisher schon intern bis rauf an den Vorstand berichten und so. Also auch hier DORA gibt ein paar neue Etiketten und DORA sagt eben klar, es muss so was geben. Aber wir haben es jetzt auch schon gefordert. Also wir haben auch jetzt in unserer aktuellen Prüfung gerade auch wieder Feststellung zum IT-Risiko Reporting, keine wahnsinnig große, aber wo wir auch sagen, gewisse Themen sind in dem einen Bericht nicht drin, sondern verstecken sich in irgendeinem anderen Untergremium. Das sollte aber auch dort hingehen, dass es der ganze Vorstand weiß. Also haben wir auch jetzt schon auch ohne DORA.

Jonathan Denzel: Und die Awareness vom Vorstand, vom Leitungsorgan zum Thema IKT Risiko?

Stefan Unteregger: Auch jetzt schon Thema. Aber da hilft DORA natürlich auch, weil medial stark präsent. Also es ist jetzt auch kein großes Geheimnis, dass in der Vergangenheit manche Vorstände nicht so wahnsinnig interessiert an den technischen Themen waren. Mit heranziehendem DORA wird auch denen klarer... Wobei man auch, also jetzt bei unseren großen Banken auch sagen muss, das ist jetzt für die auch nicht erst mit DORA. Das hatte ich jetzt schon lange nicht mehr, dass irgendwie Großbanken gesagt haben, IT ist doch eigentlich nicht so wichtig oder so. Vor 15 Jahren gab es das durchaus noch.

Jonathan Denzel: Eher im Kleinbankenbereich?

Stefan Unteregger: Bei Kleinbanken könnte ich mir vorstellen, dass es bei manchen immer noch so ist. Was dann noch mit DORA ganz neu ist, aber jetzt auch wieder für die laufende Beaufsichtigung nicht so wirklich Auswirkungen hat, ist diese ganze Sache, Critical Third Party Beaufsichtigung, also dieses Overside Framework, dass es dann dort geben wird. Das ist ja aber was, das wir uns auf sich zwar kümmern müssen, aber wo ich jetzt nicht bei der Bank prüfe deswegen. Da ist dann eher die Frage und die ist tatsächlich auch noch offen, ob und wie wir in Zukunft dann an diesem Overside Framework teilnehmen werden.

Jonathan Denzel: Okay, dann bin ich durch mit meinen Fragen. Vielen lieben Dank, dass Sie sich die Zeit genommen haben.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

List of Figures

1.1 Information security events split by sector and threat, as in [Eni23] (page 15) 3

2.1 The iterative Design Science process instantiated from Hevner et al. [HMPR04] (page 80) 9

3.1 The COBIT Core Model from ISACA [cob23] 19
3.2 The three Tier separation according to the NIST CSF [oST18] (page 12) . 21
3.3 Areas of Influence of Information Security. Source: Created by the author. 24

4.1 Different areas of resilience in the literature according to Shishodia et al. [SSRM21] (page 883) 28
4.2 Resilience evolution vs. time. From Mebarki [Meb17] (page 426) 29
4.3 Ecological resilience. Contrasting view as presented by Adger [Adg00] (page 350) 32
4.4 Supply Chain Resilience according to Shishodia et al. [SSRM21] (page 896). 34

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

List of Tables

4.1 Sorting the CD-RISC items in the triad of resilience 35

6.1 Coverage of Articles in the DORA and related RTS within the project plan template. Source: Created by the author. 54
6.2 Percentage of Articles covered by working packages in the project plan template. Source: Created by the author. 55
6.3 Coverage of controls from the ISO27001 within the project plan template. Source: Created by the author. 61
6.4 Percentage of chapters/controls covered by working packages in the project plan template. Source: Created by the author. 62
6.5 Mapping of working packages that directly mitigate the corresponding top threat. Source: Created by the author. 63

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Bibliography

[Adg00] W. Neil Adger. Social and ecological resilience: are they related? *Progress in Human Geography*, 24(3):347–364, September 2000.

[Axe19] Axelos. *ITIL Foundation: ITIL 4 Edition*. Stationery Office Books, September 2019.

[BLM09] Alexander Bogner, Beate Littig, and Wolfgang Menz. *Interviewing Experts*. 01 2009.

[BMV+19] Federica Burla, Yuval Mulla, Bart E. Vos, Anders Aufderhorst-Roberts, and Gijsje H. Koenderink. From mechanical resilience to active material properties in biopolymer networks. *Nat. Rev. Phys.*, 1:249–263, April 2019.

[CCB+20] European Commission, Joint Research Centre, G Baldini, J Barrero, G Draper, N Duch-Brown, O Eulaerts, D Geneiatakis, G Joanny, S Kerckhof, A Lewis, T Martin, S Nativi, R Neisse, D Papameletiou, J Hernandez Ramos, V Reina, G Ruzzante, L Sportiello, G Steri, S Tirendi, M Dewar, I Coisel, S Chaudron, I Nai Fovino, G Kambourakis, G Barry, B Mortara, J Sanchez, J Nordvik, H Junklewitz, and I Kounelis. *Cybersecurity, our digital anchor – A European perspective*. Publications Office, 2020.

[CD03] Kathryn M. Connor and Jonathan R.T. Davidson. Development of a new resilience scale: The connor-davidson resilience scale (cd-risc). *Depression and Anxiety*, 18(2):76–82, 2003.

[cob23] COBIT | Control Objectives for Information Technologies | ISACA, December 2023. [Online; accessed 11. Dec. 2023].

[Cou23] Payment Card Industry Security Standard Council. Official PCI Security Standards Council Site - Document, April 2023. [Online; accessed 18. Aug. 2023].

[cyb23] Infographic: Cybercrime Expected To Skyrocket in Coming Years, July 2023. [Online; accessed 17. Jul. 2023].

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

[Dem23] Schlussfolgerungen des Rates zur Rolle der Jugend bei der Bewältigung der demografischen Herausforderungen in der Europäischen Union (2018/C 196/04)-[Schl 2018/C 196/04 zur Rolle der Jugend bei der Bewältigung der demografischen Herausforderungen in der EU] - beck-online, November 2023. [Online; accessed 24. Nov. 2023].

[DRS03] Dov Dvir, Tzvi Raz, and Aaron J. Shenhar. An empirical analysis of the relationship between project planning and project success. *Int. J. Project Manage.*, 21(2):89–95, February 2003.

[DW14] Bob Duncan and Mark Whittington. Compliance with standards, assurance and audit: does this equal security? In *SIN '14: Proceedings of the 7th International Conference on Security of Information and Networks*, pages 77–84. Association for Computing Machinery, New York, NY, USA, September 2014.

[Eni23] ENISA Threat Landscape 2023, October 2023. [Online; accessed 15. Jan. 2024].

[EU-20] The EU's Cybersecurity Strategy for the Digital Decade, December 2020. [Online; accessed 27. Nov. 2023].

[EU-22] Cybersecurity: why reducing the cost of cyberattacks matters | News | European Parliament, November 2022. [Online; accessed 6. Dec. 2023].

[EU-23] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen/Schaffung einer europäischen Gesundheitsunion: Die Resilienz der EU gegenüber grenzüberschreitenden Gesundheitsgefahren stärken | Parlament Österreich, November 2023. [Online; accessed 23. Nov. 2023].

[For20] Joint Task Force. Security and Privacy Controls for Information Systems and Organizations. *CSRC | NIST*, December 2020.

[GAH09] Lance H Gunderson, Craig R Allen, and C S Holling, editors. *Foundations of ecological resilience*. Island Press, Washington, D.C., DC, August 2009.

[GGBB20] Stefan Gran, Steffi Grimm, Andreas Brieger, and Silke Brehm. Aktuelles aus brüssel und straßburg. *Arbeit und Recht*, 68(7/8):pp. 318–320, 2020.

[GHR18] Susan Gonscherowski, Marit Hansen, and Martin Rost. Resilienz – eine neue Anforderung aus der Datenschutz-Grundverordnung. *Datenschutz Datensich.*, 42(7):442–446, July 2018.

[HA04] Francis Hartman and Rafi Ashrafi. Development of the SMARTTM Project Planning framework. *Int. J. Project Manage.*, 22(6):499–510, August 2004.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

[HC10] Alan Hevner and Samir Chatterjee. *Design Research in Information Systems: Theory and Practice*, volume 22. Springer New York, 01 2010.

[HDF14] Deborah F. Hellmann, Lisa M. Dinkelborg, and Sandra Fernau. *Psychosoziale Folgen sexuellen Missbrauchs durch katholische Geistliche*, pages 185–236. Nomos Verlagsgesellschaft mbH, 1 edition, 2014.

[HDHJVG18] Tim Huygh, Steven De Haes, Anant Joshi, and Wim Van Grembergen. Answering Key Global IT Management Concerns Through IT Governance and Management Processes: A COBIT 5 View, January 2018. [Online; accessed 15. Aug. 2023].

[HHC23] Tejaswini C. Herath, Hemantha S. B. Herath, and David Cullum. An Information Security Performance Measurement Tool for Senior Managers: Balanced Scorecard Integration for Security Governance and Control Frameworks. *Inf. Syst. Front.*, 25(2):681–721, April 2023.

[HMPR04] Alan R. Hevner, Salvatore T. March, Jinsoo Park, and Sudha Ram. Design science in information systems research. *MIS Q.*, 28(1):75–105, 3 2004.

[Hol96] C. S. Holling. *Engineering Resilience versus Ecological Resilience*. National Academies Press, March 1996.

[hSIAB18] he SABSA Institute Academic Board. R101 - SABSA Matrices 2018, June 2018. [Online; accessed 21. Aug. 2023].

[Hug11] Mark Hughes. Do 70 Per Cent of All Organizational Change Initiatives Really Fail? *Journal of Change Management*, 11(4):451–464, December 2011.

[Ini11] Joint Task Force Transformation Initiative. Managing Information Security Risk: Organization, Mission, and Information System View. *CSRC | NIST*, March 2011.

[ISO22] ISO/IEC 27001 Standard – Information Security Management Systems, October 2022. [Online; accessed 15. Aug. 2023].

[KK22] Carsten Kaufmann and Alexander Kock. Does project management matter? The relationship between project management effort, complexity, and profitability. *Int. J. Project Manage.*, 40(6):624–633, August 2022.

[Kuh13] Andreas Kuhn. *Inklusion im Sozialraum aus Sicht des Deutschen Vereins*, pages 107–114. Nomos Verlagsgesellschaft mbH, 1 edition, 2013.

[Lor20] Stefanie Lorenzen. Resiliente wertschöpfungsketten per gesetz? *Arbeit und Recht*, 68(6):pp. 244–249, 2020.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

[LPL23] Ariel I. La Paz and Rodrigo I. López. Recommendation method for customized IT project management. *Procedia Comput. Sci.*, 219:1938–1945, January 2023.

[MdIdLNW23] Referat 14 Ministerium des Innern des Landes Nordrhein-Westfalen. Richtlinie über die Gewährung von Billigkeitsleistungen zur Förderung von Investitionen von Krankenhäusern zur Stärkung der Resilienz im weiteren Verlauf der Corona-Pandemie (Billigkeitsrichtlinie Corona-Sonderprogramm für Krankenhäuser) | RECHT.NRW.DE, November 2023. [Online; accessed 23. Nov. 2023].

[Meb17] Ahmed Mebarki. Resilience: Theory and metrics – A metal structure as demonstrator. *Eng. Struct.*, 138:425–433, May 2017.

[Mig23] Empfehlung (EU) 2020/1366 der Kommission vom 23. September 2020 über einen Vorsorge- und Krisenmanagementmechanismus der EU für Migration (Vorsorge- und Krisenplan für Migration) - [Empf (EU) 2020/1366/EU zu einem Vorsorge- und Krisenplan für Migration] - beck-online, November 2023. [Online; accessed 24. Nov. 2023].

[MS22] Prashant Manuja and Rajveer Singh Shekhawat. IT Security Frameworks: Risk Management Analysis and Solutions. In *ICIMMI '22: Proceedings of the 4th International Conference on Information Management & Machine Intelligence*, pages 1–7. Association for Computing Machinery, New York, NY, USA, December 2022.

[MV] Salvatore T. March and Timothy J. Vogus. Design science in the management disciplines.

[New05] Russ Newman. APA's resilience initiative. *Prof. Psychol. Res. Pr.*, 36(3):227–229, June 2005.

[Nic18] Mathew Nicho. A process model for implementing information systems security governance. *Information & Computer Security*, 26(1):10–38, March 2018.

[NIS23] Getting Started | NIST, April 2023. [Online; accessed 24. Jul. 2023].

[NLW08] E. W. T. Ngai, C. C. H. Law, and F. K. T. Wat. Examining the critical success factors in the adoption of enterprise resource planning. *Comput. Ind.*, 59(6):548–564, August 2008.

[oST18] National Institute of Standards and Technologies. Framework for Improving Critical Infrastructure Cybersecurity, April 2018.

[PdK23] PdK Bay G-2 | AVBayKiBiG 1. Abschnitt - beck-online, November 2023. [Online; accessed 23. Nov. 2023].

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

[PK23] Jeffrey Phillips and James D. Klein. Change Management: From Theory to Practice. *TechTrends*, 67(1):189–197, January 2023.

[PLS20] Hanna Paananen, Michael Lapke, and Mikko Siponen. State of the art in information security policy development. *Computers & Security*, 88:101608, January 2020.

[Rat23a] Schlussfolgerungen des Rates zu einer Strategie der EU für die internationalen Kulturbeziehungen (2017/L 189/08)-[Schl 2017/C 189/08 zur Strategie für die internationalen Kulturbeziehungen] - beck-online, November 2023. [Online; accessed 24. Nov. 2023].

[Rat23b] Schlussfolgerungen des Rates zum Risikomanagement im Bereich des Kulturerbes (2020/C 186/01) - [Schl 2020/C 186/01 zum Risikomanagement im Bereich des Kulturerbes] - beck-online, November 2023. [Online; accessed 24. Nov. 2023].

[Res23a] Bechtold/Bosch/Brinker | Vertikal-LL - beck-online, November 2023. [Online; accessed 24. Nov. 2023].

[Res23b] Krenzler/Herrmann/Niestedt | VO (EU) 2022/2560 Präambel, Erwägungsgründe - beck-online, November 2023. [Online; accessed 24. Nov. 2023].

[Res23c] resilience | Etymology, origin and meaning of resilience by etymonline, July 2023. [Online; accessed 17. Jul. 2023].

[SCL09] John Sherwood, Andrew Clark, and David Lynas. Enterprise Security Architecture - Whitepaper, January 2009. [Online; accessed 21. Aug. 2023].

[SD21] Hélène Sicotte and Hélène Delerue. Project planning, top management support and communication: A trident in search of an explanation. *J. Eng. Tech. Manage.*, 60:101626, April 2021.

[SHB17] Falko Stetter and Sabine Heukrodt-Bauer. IT-Grundschutzkataloge des BSI — Last oder Mehrwert? *Wirtsch. Inform. Manag.*, 9(4):62–66, August 2017.

[Sny19] Hannah Snyder. Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104:333–339, 08 2019.

[SOC23] SOC 2®, July 2023. [Online; accessed 24. Jul. 2023].

[Sol21] Cyberangriff auf die USA eskaliert immer weiter - fm4.ORF.at, January 2021. [Online; accessed 15. Jan. 2024].

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

[SP821] NIST SP 800-30 | NIST, April 2021. [Online; accessed 18. Aug. 2023].

[SSRM21] Anjali Shishodia, Rohit Sharma, R. Rajesh, and Ziaul Haque Munim. Supply chain resilience: A review, conceptual framework and future research. *International Journal of Logistics Management*, 34(4):879–908, December 2021.

[Str24] The Fed - SR 20-24: Interagency Paper on Sound Practices to Strengthen Operational Resilience, August 2024. [Online; accessed 5. Oct. 2024].

[Tah22] Hamed Taherdoost. Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. *Electronics*, 11(14), 2022.

[Tal07] Nassim Nicholas Taleb. 'The Black Swan: The Impact of the Highly Improbable'. *N.Y. Times*, April 2007.

[TDD14] Frosina Tasevska, Talib Damij, and Nadja Damij. Project planning practices based on enterprise resource planning systems in small and medium enterprises — A case study from the Republic of Macedonia. *Int. J. Project Manage.*, 32(3):529–539, April 2014.

[Thu84] R.H. Thurston. *The materials of engineering*. New York: John Wiley & Sons, 1884.

[Tur10] Daniel Turner. Qualitative interview design: A practical guide for novice investigators. *Qualitative Report*, 15, 05 2010.

[VE07] A. Da Veiga and J. H. P. Eloff. An Information Security Governance Framework. *Information Systems Management*, 24(4):361–372, October 2007.

[VLG22] João Varajão, João Carlos Lourenço, and João Gomes. Models and methods for information systems project success evaluation – A review and directions for research. *Heliyon*, 8(12):e11977, December 2022.

[WBN11] Gill Windle, Kate M. Bennett, and Jane Noyes. A methodological review of resilience measurement scales. *Health and Quality of Life Outcomes*, 9(1):8, Feb 2011.

[WD21] Andreas Wieland and Christian F. Durach. Two perspectives on supply chain resilience. *J. Bus. Logist.*, 42(3):315–322, July 2021.

[Wil17] Helmut Willke. Demokratie im umbruch. *Der Staat*, 56(3):357–387, 2017.

[WXY+23] Yujie Wang, Jixiang Xu, Shitong Yang, Junjia Jiang, and Junling Gao. Exploratory graph analysis on the Connor–Davidson Resilience Scale (CD-RISC) among older adults in China. *Sci. Rep.*, 13(19971):1–12, November 2023.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

[Ös23] Wirtschaftskammer Österreich. Digital Operational Resilience Act (DORA), March 2023. [Online; accessed 31. Jul. 2023].

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.