FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Integrated Enterprise Risk and Resilience Management

A Cybernetic Planning and Control Framework

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Wirtschaftsingenieurwesen Informatik

eingereicht von

Armin Preis, BSc
Matrikelnummer 9830073

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung: Univ. Prof. Mag. rer. soc. oec. Dr. rer. soc. oec. Walter Schwaiger, MBA

Wien, 01.10.2013

(Unterschrift Verfasser) (Unterschrift Betreuung)

FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Integrated Enterprise Risk and Resilience Management

A Cybernetic Planning and Control Framework

MASTER'S THESIS

submitted in partial fulfillment of the requirements for the degree of

Diplom-Ingenieur

in

Business Engineering and Computer Science

by

Armin Preis, BSc
Registration Number 9830073

to the Faculty of Informatics
at the Vienna University of Technology

Advisor: Univ. Prof. Mag. rer. soc. oec. Dr. rer. soc. oec. Walter Schwaiger, MBA

Vienna, 01.10.2013

(Signature of Author) (Signature of Advisor)

Erklärung zur Verfassung der Arbeit

Armin Preis, BSc
Hackinger Straße 43/27, 1140 Vienna

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.

(Ort, Datum) (Unterschrift Verfasser)

Acknowledgements

In deep gratitude and love for Kristina, Roswitha, Alexandra and Albert.

I want to thank Univ. Prof. Mag. Dr. Walter Schwaiger for his tremendous inspiration in the field of management cybernetics and for his professional support by means of research supervision and constructive discussions.

Abstract

Context of the Thesis The postmodern socioeconomic system is coined by an unprecedented interdependency of organizations around the whole globe. Companies have to face external systemic risks they can not influence. They have to become more resilient to survive crises and more efficient to stay successfully in business under the pressure of worldwide competition at the same time.

Goal of the Thesis The goal of this thesis is to develop a cybernetic risk and resilience management framework that allows to plan and control internal risks and to prepare for external risks so that a more competitive business strategy can be applied. The framework shall include (1) *a cybernetic steering model*, (2) a description of necessary *resilience and risk management activities* and (3) and an overview over the *flow of involved information*. The overall goal is to provide a handbook for managers who want to establish, run and control an integrated risk and resilience management in organizations.

Methodology The scientific research approach is the *Design Science Methodology* that is divided into three major parts. The first one is a *literature analysis on risk and resilience management* to evaluate current standards and trends in these management domains. The second part is a detailled analysis of the most mature risk and resilience management standards in order to *model* them as *cybernetic risk and resilience management frameworks*. The integration of the developed management frameworks into a *cybernetic enterprise wide risk and resilience management framework* as well as an evaluation, whether the developed artifacts provide added value for risk and resilience managers, constitute the final part of the research process.

Results As first result, the ISO 31000 Risk Management Standard and the ASIS Organizational Resilience Management Standard were modeled as *Cybernetic Risk* and *Resilience Management Frameworks*. As second result, the integration of existing management approaches into the new *Recursive Cybernetic Management Model (RCMM)* was conducted. The RCMM constitutes the basis for the integration of the two developed Cybernetic Management Frameworks into the final research result, the *Enterprise Resilience Management Meta-Framework (ERM-MF)*. The ERM-MF facilitates the steering of enterprise resilience by managing risks on and resilience of assets as well as the quality of management processes.

Kurzfassung

Kontext Das postmoderne sozioökonomische System ist geprägt von einer noch nie da gewesenen Interdependenz moderner Organisationen auf der ganzen Welt. Unternehmen stehen systemischen Risiken gegenüber, welche sie auf keinste Weise beeinflussen können. Sie sind gezwungen, gleichzeitig resilienter zu werden, um systemische Krisen zu überleben, und effizienter zu werden, um unter dem Druck der globalen Konkurrenz unternehmerisch erfolgreich zu bleiben.

Ziel der Arbeit Das Ziel dieser Arbeit ist, ein integriertes, kybernetisches Risiko- und Resilienzmanagement Framework zu entwickeln. Dieses Framework soll Unternehmen ermöglichen, interne Risiken zu steuern und sich auf externe Risiken bestmöglich vorzubereiten. Es soll Unternehmern erlauben, konkurrenzfähige Geschäftsstrategien umzusetzen, ohne sich dem Risiko des unternehmerischen Untergangs auszusetzen.

Wissenschaftliche Methode Der wissenschaftliche Ansatz der Arbeit basiert auf der Design Science Methodologie. Der Forschungsprozess besteht aus drei aufeinander aufbauenden Teilen. Der erste beinhaltet eine Analyse von Risiko- und Resilienzmanagement Literatur, um die Anforderungen an ein neues Managementmodell zu erheben. Im zweiten Teil werden die analysierten Management Standards als kybernetische Risiko- und Resilienzmanagement Frameworks modelliert. Im letzten Teil werden die entwickelten Modelle zu einem unternehmensweiten Management Metaframework integriert und evaluiert, um sicherzustellen, dass das entwickelte Metaframework den geforderten Nutzen für Manager bringt.

Ergebnisse Der ISO 31000 Risiko- und der ASIS Resilienzmanagement Standard wurden als kybernetische Frameworks modelliert. Durch die Integration bestehender Managementtheorien konnte das neue *Rekursive Kybernetische Managementmodell (RCMM)* entwickelt werden. Auf der Grundlage des RCMM wurden die zwei entwickelten kybernetischen Prozessmodelle in das neue Unternehmensweite Resilienzmanagement Metaframework *(ERM-MF)* integriert. Dieses Steuerungsmodell erlaubt, sowohl Risiken, als auch die Qualität von Managementprozessen, zu messen und die Resilienz von Unternehmen integriert zu steuern.

Contents

1 Introduction **1**
- 1.1 Motivation . . . 1
- 1.2 Problem Statement . . . 2
- 1.3 Aim of the Thesis . . . 3
- 1.4 Relevance . . . 4
- 1.5 Structure of the Thesis . . . 5

2 Methodology **7**
- 2.1 Used Concepts . . . 7
- 2.2 Research Questions . . . 13
- 2.3 Methodological Approach . . . 13

3 Risk Management **19**
- 3.1 Risk Management Models . . . 19
- 3.2 Current Trends in Risk Management . . . 24
- 3.3 Prevalent Problems in Enterprise Risk Management . . . 27
- 3.4 Key Findings . . . 29

4 Resilience Management **31**
- 4.1 Organizational Resilience . . . 31
- 4.2 Resilience Management Models . . . 38
- 4.3 Key Findings . . . 43

5 Development of an Enterprise Risk and Resilience Management Framework **45**
- 5.1 Cybernetic Risk Management Framework . . . 46
- 5.2 Cybernetic Resilience Management Framework . . . 57
- 5.3 Comparison of Risk and Resilience Management . . . 69
- 5.4 Integrated Enterprise Risk and Resilience Management Framework . . . 72

6 Critical Reflection **85**
- 6.1 Evaluation of the Developed Meta-Framework . . . 85
- 6.2 Comparison with Related Work . . . 88
- 6.3 Discussion of Open Issues . . . 89
- 6.4 Conclusion . . . 90

7 Summary and Future Research **91**
7.1 Summary 91
7.2 Future Research 92

Bibliography **95**

A Tables Appendix **101**
A.1 Stephenson's Indicators of Organizational Resilience 101
A.2 Comparison of ASIS Resilience Management Activities with CERT Resilience Metrics 103
A.3 Comparison of ISO 31000 Risk Management Activities with CERT Resilience Metrics 113

List of Figures

2.1 The PDCA-Cycle or Deming Wheel 8
2.2 Anthony's Planning and Control Framework 9
2.3 Schwaiger's Cybernetic Management Framework 10
2.4 The CMF-Cube 11
2.5 The General Model of Systemic Control (MSC) 12
2.6 The Information System Design Science Framework 14
2.7 Methodological Approach for the Thesis 16

3.1 The COSO-Cube 21
3.2 The ISO 31000 Risk Management Components 23
3.3 The ISO 31000 Risk Management Processes 24
3.4 The Risk Culture Aspects Model 26
3.5 Tentative Conceptual Model of Risk Culture 28

4.1 Resilient and Rigid Crisis Response 33
4.2 Processes for Mindfulness 36
4.3 ASIS Organizational Resilience Management System Flow Diagram 39

5.1 The ISO 31000 Risk Management Process Modeled as Cybernetic Management Framework 47
5.2 The ISO 31000 Risk Management Ontology 50
5.3 The ASIS Resilience Management Standard Modeled as Cybernetic Management Framework 58
5.4 ASIS Organizational Resilience Management Ontology 63
5.5 The Phases of Resilience Management 71
5.6 Integrated Functional Model of Resilience Management 71
5.7 The Recursive Cybernetic Management Model (CRMM) 74
5.8 The Recursive Cybernetic Management Model and its Environments 76
5.9 Enterprise Resilience Management Meta-Framework (ERM-MF) 78
5.10 A Composite Model of Enterprise Resilience Management (CM-ERM) 81

List of Tables

3.1 Goals and Principles of the ISO 31000 Risk Management Standard 23

4.1 Process Areas of the CERT Resilience Management Model 41

5.1 Selection of CERT-RMM Process Areas that Comply with the ASIS and ISO 31000 Management Activities 80

6.1 Evaluation of the Developed Meta-Framework 87

A.1 Stephenson's Indicators of Organizational Resilience 102
A.2 Matching of CERT-RMM Specific Practices, Metrics and ASIS Resilience Management Activities 112
A.3 Matching of CERT-RMM Specific Practices, Metrics and ISO 31000 Risk Management Activities 114

CHAPTER 1

Introduction

" If you want to create change, you must challenge not only the models of unreality, but the paradigms that underwrite them. "

[Anthony Stafford Beer, 1926 - 2002.]

Contents

1.1 Motivation **1**
1.2 Problem Statement **2**
1.3 Aim of the Thesis **3**
1.4 Relevance **4**
1.5 Structure of the Thesis **5**

1.1 Motivation

The *resilience of organizations*[1] is an emerging topic of interest, especially since the global financial crisis unearthed the strong interdependency of modern organizations. They have to perform in an increasingly interconnected economy and cope with extreme complex and fast changing environments. Not only the global economic dependency on other organizations, but also the realization of systemic ecological, technological and human risks can have strong negative impact on any organization.

The scientific community revealed that the realization of these systemic risks has the highest probability of disrupting and destroying organizations and whole socioeconomic networks.

[1] In this context *resilience* is the capability of an organization to recover from any kind of negative impact or crisis. The concept of resilience is better known in the psychological or ecological research area where it signifies the ability of a person or system to recover from a crisis. The semantic roots of 'resilience' lie in the latin word 'resilio' which means 'to rebound'.

Even the World Economic Forum emphasizes that these critical system failures represent the most hazardous type of risk companies have to face in the economic and technological environment [2013, pp. 46-47]. Fischbacher and Smith from the Glasgow University call these hazards *borderless risks*, as they are generated across different tangible and intangible borders [2009, p. 3]. The rise of these borderless risks transformed the identification and treatment of risks into a central management domain in large organizations. In spite of this trend towards enterprise risk management (ERM), the recent financial crisis killed the game of enterprise risk management out of the blue. The crisis uncovered that existing risk management systems can either not predict or at least not prevent the realization of risks in a way it would be necessary. As a consequence, Kaplan and Mikes, researchers at the Harvard Business School, conducted intense case study research on existing enterprise risk management systems and its industrial application. They found that the use of wide-spread enterprise risk management frameworks does not inherently increase the capability of overcoming hazards that arise from the realization of external risks [2012; 2013].

No matter, whether the reason for the ineffectiveness of ERM systems lays in its design, in its implementation, in cultural or human aspects of management, it has become clear that a revision of ERM systems is inevitable to find out how its effectiveness can be improved. Kaplan and Mikes propose to enlarge existing ERM systems in a way that empowers managers to better prepare for external events [2012; 2013]. Power, researcher at the London School of Business, comes to a similar research result. He found that risk management in enterprises is predominantly shaped by a quantitative management paradigm that is not capable of recognizing the complexity of risks that arise outside of a firm's border [2009]. He proposes to enlarge ERM systems with business continuity management, the same way as Price Waterhouse Coopers do [2009], to increase the probability of successfully dealing with risks realized a hazardous impact on the organization. Last but not least, the World Economic Forum recommends to focus on the broader concept of resilience management, than on pure mathematical approaches, to increase the organizational capability of adjusting to a rapidly changing environment.

In summary, several economic authorities like the World Economic Forum [2013], Hamel and Valikangas [2003] state organizational resilience management to be the most promising foundation for a new risk-integrated enterprise steering model.

1.2 Problem Statement

Up to now, there exists no meta-framework or *cybernetic*[2] framework that could serve as guidance for organizations or enterprises before, during and after the realization of risks in terms of various types crises. Such a meta-framework that is at the same time applicable for small organizations and expandable for large enterprises would relief the navigation at heavy sea of globalized economics.

[2] *Cybernetics* is the science of steerage [Beer, 1972] introduced by Wiener as 'the science of control and communication in the animal and the machine' [1963]. Foerster [2003] expanded the theory to the *second order cybernetics* by introducing an observer that observes a first order system what allows adaptive learning within any technological, biological or sociological system.

The only encompassing organizational resilience management models are the ASIS SPC.1-2009 Organizational Resilience Management Model [Blass, 2010] and the CERT Resilience Management Model [Caralli et al., 2010a]. All other existing models concentrate either on risk management, business continuity management or on crisis management. The CERT model is constituted by a collection of several hundred resilience management activities and related process capability metrics. This approach is not suitable as meta steering model for managers that do not have a lot of experience in resilience management, as it is a very extensive collection of processes and metrics, but not a steering or meta model. The ASIS model incorporates the PDCA-Cycle, that will be introduced in the next chapter on used concepts for this thesis, and would therefore generally be usable as steering model. However the ASIS model includes about sixty pages of mostly plain text what makes it difficult for managers to extract the different planning and control cycles in dependence of internal and external events.

1.3 Aim of the Thesis

The main aim of the thesis is to evaluate whether a *framework for integrated enterprise risk and resilience management* in the sense of Schwaiger's Cybernetic Management Framework (CMF) [2012] can be developed. The achievement of the expected aim is split up into two distinct subgoals that lead to the answer of the main aim in accordance with the methodology that will be presented in Chapter 2. The utilization of the CMF as basis for the modeling of a meta-framework makes it possible to provide a visual representation that can be used as a steering model that is still missing in this management domain.

Subgoal one is an evaluation of whether risk management can be modeled as cybernetic management framework. If risk management can be modeled as CMF, the modeling is conducted and visualized in a comprehensive way including all necessary data-objects, risk management activities, the flow of information, as well as the management cycles within the CMF. Subgoal two is an evaluation of whether organizational resilience management can be modeled as cybernetic resilience management framework. If the risk management can be modeled as CMF this is, again, conducted and visualized in a comprehensive way including all necessary data-objects, risk management activities, the flow of information, as well as the planning and control cycles within the CMF.

If subgoals one and two are reached during in the course of the thesis, an evaluation of whether the developed risk management framework and the resilience management framework can be integrated into one enterprise-wide cybernetic risk and resilience management meta-framework, as defined as main aim, can be conducted. If the integration is possible, it is conducted and visualized by the same means that were used in the previous modeling sections. The cybernetic meta-model for integrated risk and resilience management integrates the flow of activities, information and control cycles through all hierarchy-levels of an organization.

If the development of the integrated cybernetic eneterprise-wide risk and resilience management framework will be successful, the thesis will add a *central theoretic contribution to the revision of enterprise risk management and to the integration of the risk and resilience management paradigms*. If the integration fails, it will add valuable scientific knowledge in the sense of

Popper's positive rationalism.[3] No matter, whether the evaluation shows that the integration can be done or not, the aim of the thesis is not to prove the validity of the developed theory in an empirical way, as it would transcend the sensible effort for this thesis. Nevertheless, the provided theoretical concept will serve ase working hypothesis for future research efforts, empirical case studies and evaluations.

1.4 Relevance

Enterprise risk management has become a major topic for large firms, especially in the United States of America and the European Union. In these regions legislation has imposed new regulations concerning the internal control and risk management in firms.[4] Organizations have to build up an efficient internal control and risk management mechanism. The Committee of the Sponsoring Organizations of the Treadway Commission was the first organization that introduced an internal control framework, named COSO. Since there, the concept was overworked and improved in a continuous way. The intense work on this topic resulted in the COSO II Integrated Enterprise Risk Management Framework [2004] and in the updated, even more comprehensive, Internal Control Framework [2013]. Besides COSO, different standardization organizations and professional associations dealt with the topic of risk management. The Federation of European Risk Management Associations was one of the first who published a generic risk management standard [2002] and the International Standardization Institution developed the ISO 31000 Risk Management Standard [2009].

The concept of *organizational resilience* arose within the last fifteen years. Researchers have tried to explain why some organizations successfully recover from negative impacts and crises, whereas others perish under similar adverse conditions. The first researchers shaping the concept of resilience in organizational sciences were Weick et al. [2008]. They had focused their research on high reliability organizations and developed a first idea of organizational resilience [2003]. The organizational resilience research is rather young, hence most research results are qualitative ones basing on case studies and expert interviews [McManus, 2008; Stephenson, 2010; Weick, 1993]. These studies brought up core elements and indicators of resilient enterprises.

First industrial organizations jumped on the bandwagon of the resilience concept and developed *resilience management models*. The major models are the ASIS Organizational Resilience Management Standard [Blass, 2010] that incorporates a structured re- and proactive approach for preventing risks and for preparing on their realization. The Software Engineering Institute at the Carnegie Mellon University is well known for its standards on process capability and maturity. The institute developed a process capability model for operational resilience management, called the CERT Resilience Management Model (RMM) [Caralli et al., 2010c]. This model contains hundreds of organizational resilience management activities and metrics for measuring the capability of resilience management processes. An overview over the development of the term resilience in different fields of research can be found in Bhamra et al. [2011].

[3] Following Karl Popper's definition of positive rationalism, scientific knowledge-gain bases on hypotheses that must be falsifiable in empirical experiments.

[4] Details on the legislation forcing enterprises to conduct serious internal control and risk management follow in Chapter 3.

Although, there arise claims for the integration of enterprise risk management with complementary techniques like business continuity management, crisis management or resilience management, there exist no models that perform the required integration on a cybernetic level. The target of this thesis is to provide a first integrated meta-model.

1.5 Structure of the Thesis

Chapter 2: Methodology This chapter provides information on the methodology of the thesis. After a short introduction into used concepts like cybernetic management the research questions, the structure and the course of the scientific analysis method as well as the justification for the chosen methodology are being presented.

Chapter 3: Risk Management This chapter represents a literature analysis on the theory of enterprise risk management. The focus lies on widely diffused and accepted standards like the COSO II and the ISO 31000 risk management standards and current trends in enterprise risk management.

Chapter 4: Resilience Management In this chapter a second literature analysis introduces research results on organizational resilience with strong empirical evidence and existing models for resilience management.

Chapter 5: Development of an Enterprise Risk and Resilience Management Framework The core analysis and development of a solution for integrated cybernetic risk and resilience management is presented in this chapter. The analysis includes a separated examination of risk management and resilience management as first phase introspection. The development of cybernetic management frameworks and the integration of risk and resilience management into one framework is done in the second phase.

Chapter 6: Critical Reflection The reflection focuses on strengths and weaknesses of the used methodology and the developed solution. A discussion of open issues and a comparison with related work completes the chapter.

Chapter 7: Summary and Future Research This chapter offers a structured summary of the thesis and a summary of the research findings. As conclusion for the whole thesis ideas for further research are presented and discussed in a brief way.

CHAPTER 2

Methodology

" We have to remember that what we observe is not nature herself, but nature exposed to our method of questioning. "

[Werner Karl Heisenberg, 1901 - 1976.]

Contents

2.1 Used Concepts **7**
2.2 Research Questions **13**
2.3 Methodological Approach **13**

Abstract The goal of this chapter is to provide a short introduction into the concepts the later analysis will build up upon. The core research methodology, research questions and the justification for the choice of the methodological research approach are explained.

2.1 Used Concepts

This section includes an introduction in to the theoretical concepts that will be referred to and used in the different parts of the thesis.

2.1.1 The Generic Cybernetic Management Framework

Schwaiger [2012] developed a generic *Cybernetic Management Framework (CMF)* that can be applied to any management domain. The framework bases on the *(1) feedback principle, the (2) control and communication principle* of traditional cybernetics [Wiener, 1963] and on the *(3) double loop principle* of second order cybernetics [Foerster, 2003]. He integrates all three principles into a new object- and process-oriented management framework where "all operational

and managerial activities are modeled together with the corresponding information flow", [2012, p. 442]. Schwaiger visualizes the new management concept as activity diagram that includes all management and operational levels of an enterprise, as illustrated on Figure 2.3. This concept facilitates the development of a cybernetic management framework for any management field, like risk management, human resources management, or financial management, and the a seamless integration into enterprise management systems.

The first core element of the cybernetic management framework is the *Plan-Do-Check-Act Cycle (PDCA-Cycle)* (see Figure 2.1), or Deming-Wheel [Deming, 2000] that is, according to Schwaiger, "the operating principle of ISO's management system standards", [2012, p. 428].

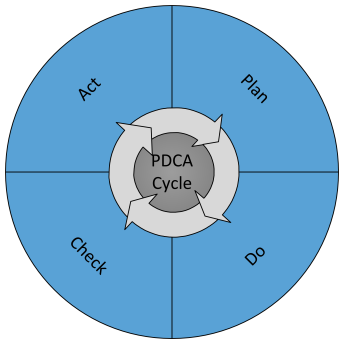

Figure 2.1: The PDCA-Cycle or Deming Wheel

The second core element of the CMF is the managerial *Planing and Control Framework (PCF)* developed by Anthony [1965]. Anthony divided business management into a *planning system*, a *control system*, and *an operating system*. Schwaiger put the depicted PDCA-Cycle into the new Planning and Control Framework and provided a structured basis for applying the Deming-Wheel to hierarchical management systems [2012]. This makes the management cycle run through distinct but overlapping management systems and hierarchies to form an integrated management cycle. Figure 2.2 illustrates the elements of the Planning and Control Framework.

Schwaiger uses Anthony's Framework as hierarchical basis, with the *Planning System* on the top, the *Control System* in the middle and the *Operating System* on the bottom, as depicted on Figure 2.3.

Schwaiger utilizes further aspects of first and second order cybernetics to refine the Deming Wheel running through the three depicted subsystems, as briefly explained in the following. The activities in the CMF are modeled as rounded rectangles. The central management activities are the *plan-activity (1)*, the *check-activity (2)* and the (3) *act-activities (4, 5)* while the operation of business processes is called *do-activity*. Information entities that are used to transfer information from one activity or system to another are modeled as rectangles. The CMF includes several distinct subsystems or control-cycles that are specified in the paragraphs below.

Subsystems of the Cybernetic Management Framework

First Order Closed Loop Control System Each organization has performance goals that are part of the CMF as the entity called *standard of performance (1a)*. These goals are compared

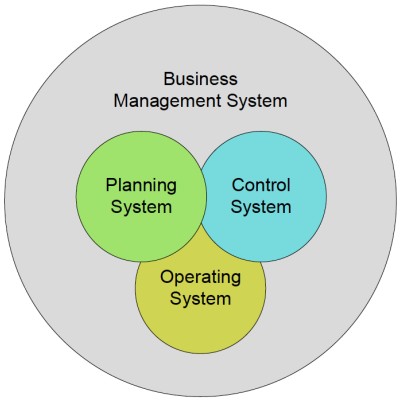

Figure 2.2: Anthony's Planning and Control Framework

In Accordance with Schwaiger [2012].

to the actually realized performance of a business process *realization (2a)* in the *check-activity (3)*. The resulting deviation is evaluated in accordance with the *control rules (1d)* and treated in the *corrective act-activity (4)* what results in the *corrective control input (4a)* for the business system. This cycle is called the *First Order Closed Loop Control System* as objectives were set within the system and the realized performance of the system is evaluated in comparison to the set objectives. First order refers in this context to the first order cybernetics.

Second Order Closed Loop Control System If the deviation is treated in the *adaptive act-activity (5)* in accordance with the *adaptive act rules (1e)*. The resulting *control input (5a)* is handled back to the planning system as input for re-planning. This cycle is called the *Second Order Closed Loop Control System* as it facilitates and incorporates second order or double loop learning for an organization, introduced by Argyris [1977].

First Order Open Loop Control System The realization of the *state variable (2b)* is not compared to any objectives. The realization does not depend on enterprise-internal business processes. In contrary, the state variable is an observation of something happening outside the company. Therefore, it goes directly into the *corrective act-activity (4)* without any comparison to company objectives. The result is the *control input (4b)* that aims to change the enterprise-internal business processes as reaction to some external events. This control cycle is called the *First Order Open Loop Control System*. The term *open* signifies that the control system is an open one and does react to events happening outside the system-boarder, the boarder of the enterprise or organization.

Second Order Open Loop Control System The realization of the *state variable (2b)* can also be evaluated in the *adaptive act-activity (4b)* what results in the *control input* for the *Planning System*. This system permits, again, adaptive second order learning for the organization, but this

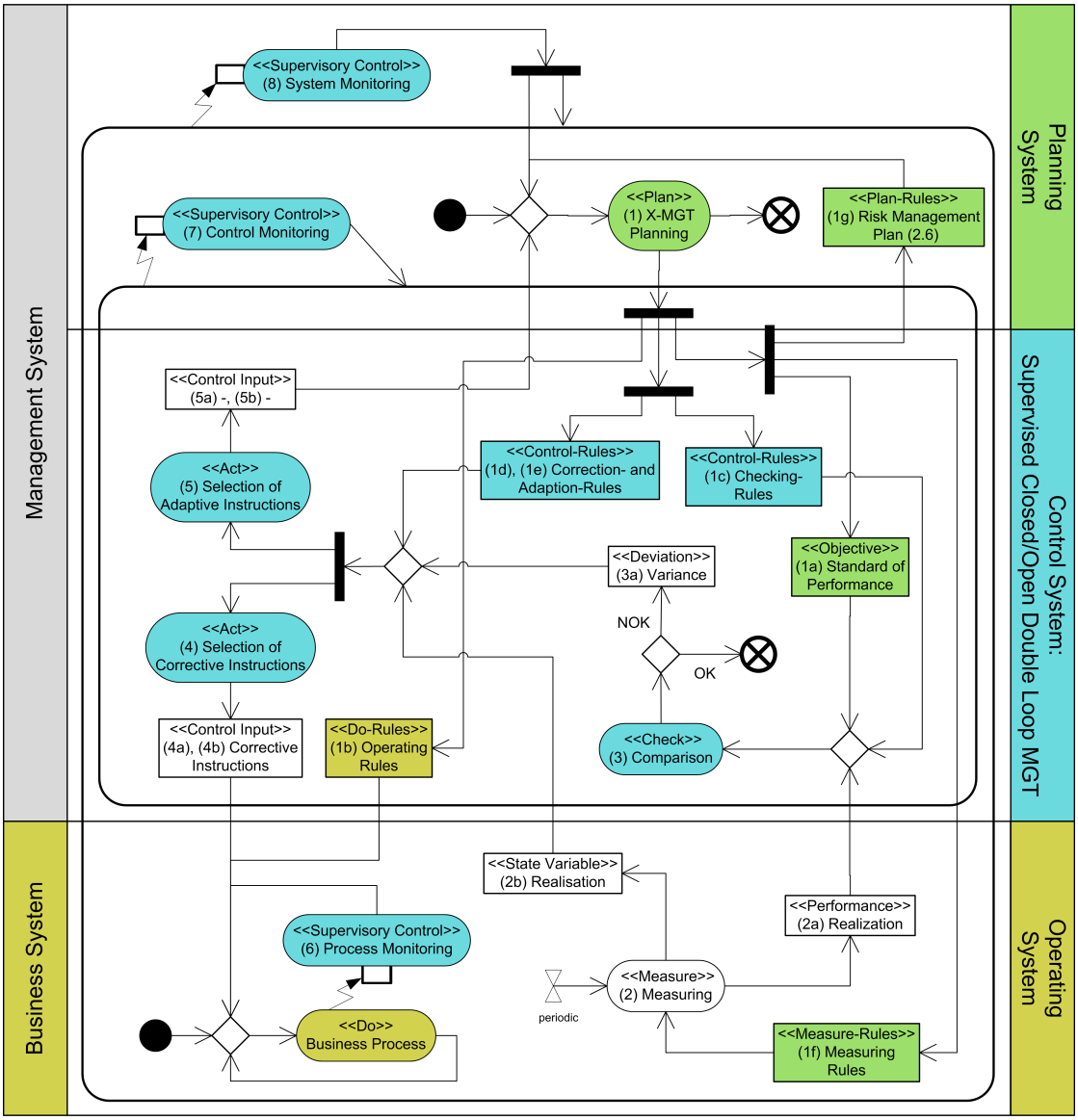

Figure 2.3: Schwaiger's Cybernetic Management Framework

In Accordance with Schwaiger [2012].

time dependent on the observation of external events. This system is called *Second Order Open Loop Control System*

It becomes clear that the CMF is a rather complex framework, that involves all central ideas of the cybernetic management paradigm, originally introduced by Beer [1972]. Schwaiger adduces that the closed loop control system can be used to control simple level three systems out of Boulding's *Levels of System Complexity* [Boulding, 1956; Schwaiger, 2012]. However, the self-

reflection principle of the second order cybernetic system is necessary to control “level seven to nine systems” of Boulding’s hierarchy [Schwaiger, 2012, p. 432]. The self reflection allows the whole system to realize necessities for changes - due to internal or external events - in the structure, the processes, or the subsystems.

Proactivity and Reactivity

Each of the four subsystems of the CMF can either be proactive or reactive. Reactive means, that planned values are compared with actually realized values [Schwaiger, 2012, p. 447], whereas proactive means that “the measured information is transformed into future related information [like forecasts].”, [Schwaiger, 2012, p. 433].

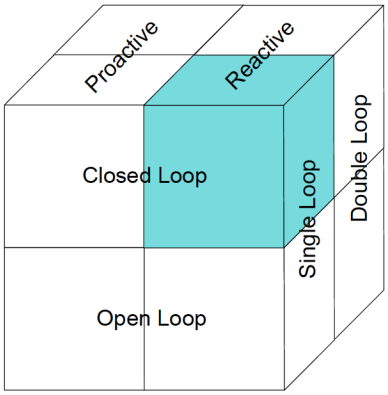

Figure 2.4: The CMF-Cube

Source: [Schwaiger, 2012]

Combining the pro- and reactivity approach with the four subsystems, eight distinct types of subsystems can be found. Schwaiger visualizes this as three-dimensional cube in Figure 2.4. In the figure he marks the simplest possible configuration of the subsystem: *a Reactive Single-, Closed-Loop Control System*.

Enforcement Rules

Schwaiger adduces a core problem within planning and control systems called the problem of organizational control [Schwaiger, 2012, p. 434]: An enterprise involves a large number of persons that fulfill different roles. However, each person has self interests what leads to the problem that employees not alway behave as they are expected to. As solution for this problem organizations use *operating rules* and *enforcement rules*. Operating rules instruct members of the organization on how to act and enforcement rules shall persuade them to act according to the operating rules. This management paradigm, developed by Arrow [1964], is also know under the terms *control in the large*, what means the use of operating rules, and *control in the small*,

what means the use of enforcement rules including detection of deviation in behavior as well as punishment [Schwaiger, 2012, p. 434].

In the CMF the *operating rules* are results of the *planning-activity (1)*, whereas, the *supervisory enforcement rules* are implemented in three distinct supervisory control activities: *process monitoring (6), control monitoring (7)*, and *system monitoring (8).*

The CMF framework will be used as underlaying concept for the modeling of risk and resilience management frameworks in the second step of the research process, namely the development of cybernetic steering models in Chapter 5.

2.1.2 The General Model of Systemic Control

The General Model of Systemic Control (MSC) is a further management model that will be referred to in the course of the thesis. Schwaninger, the developer of this model, tells the history of its development the following way: in contrast to many business schools that "were organized along disciplinary lines (i.e. the chairs, research groups and institutes specialized in certain functions such as production, marketing, personnel, etc.) or methodological compounds (e.g. decision making, organizing, accounting)", [2001a, p.1210], the University of St. Gallen introduced a generalist outlook on management. On the basis of a broad, systemic management approach, the first version of the strongly diffused "St. Gallen Management-Modell" evolved. This model focuses on the interrelation between the firm an its environment including stakeholders, economic, technological, and social spheres as well as the ecological domain [Schwaninger, 2001a, pp. 1211–1212]. Basing on this systemic approach, Schwaninger et al. elaborated a new *General Model of Systemic Control (MSC)* that grounds on organizational cybernetics and shows the interrelations between the three management levels. The MSC is illustrated in Figure 2.5.

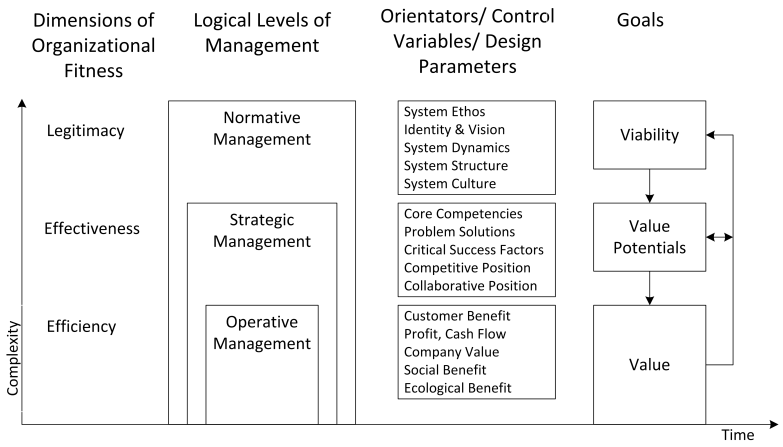

Figure 2.5: The General Model of Systemic Control (MSC)

In Accordance with Schwaninger [2001a, p. 1216].

Figure 2.5 illustrates clearly the logical levels of management: *(1) Normative, (2) Strategic* and *(3) Operative Management* and the related goals, control variables, as well as dimensions

of organizational fitness. The hierarchically allocated dimension of organizational fitness is a strong link to the concept of organizational resilience and will simplify the integration of the MSC, the CMF and resilience management approaches in later phases of the research process.

2.2 Research Questions

RQ 1 How does the scientific and industrial management community define risk, risk management and enterprise risk management?

RQ 2 How does the scientific and industrial management community define organizational resilience and organizational resilience management?

RQ 3 Which activities, information and information-flow shall a cybernetic management framework for risk-management include?

RQ 4 Which activities, information and information-flow shall a cybernetic management framework for resilience management include?

RQ 5 What is the difference between risk management and resilience management concerning activities, information-flow, and cybernetic management levels?

RQ6 How can risk management and resilience management be integrated into one cybernetic enterprise management framework?

2.3 Methodological Approach

The aim of the thesis is to provide meta-steering-models for risk and resilience management. This meta-analysis requires an abstract view on the business and management domain which (1) allows to abstract the core elements of successful management and (2) provides a clear and integrated view on all information-entities, processes, resources and flow of control. The quest for a research methodology that fulfills these requirements ended in the research field of Design Science.

2.3.1 Design Science in Information System Research Approach

Design Science in Information System Research has the aim to improve the efficiency and effectiveness of organizations. The improvement is provided by modeling organizations and providing new abstract models of the organization. These models can be implemented as information systems supporting the effectiveness and efficiency of a whole organization [Hevner, 2004, p. 76].

According to Hevner, there exist two prevailing paradigms in the field of information system research. The first one is the behavioral science paradigm that seeks to predict human and organizational behavior [2004, p. 75]. The second one is the Design Science paradigm that has the goal to “extend the boundaries of human and organizational capabilities by creating new and innovative artifacts”, [2004, p. 75]. The methodological basis of this thesis is the Design Science

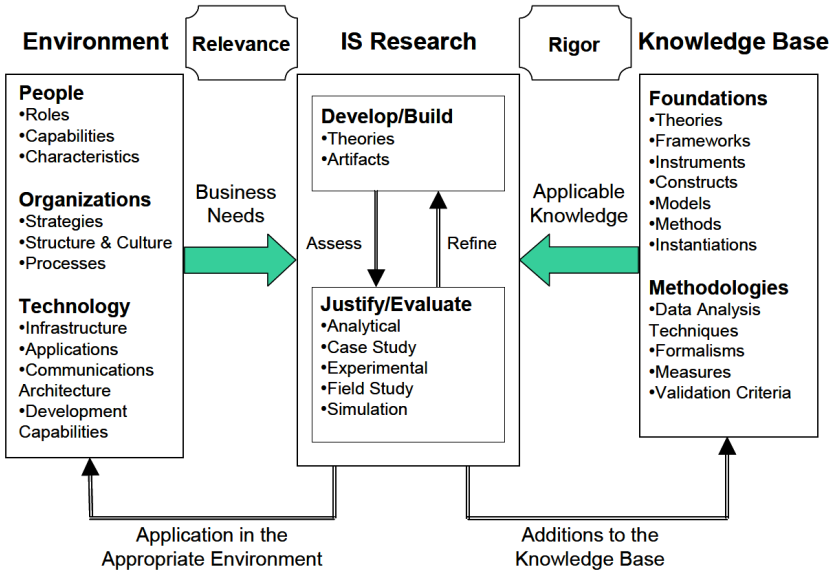

Figure 2.6: The Information System Design Science Framework

Source: [Hevner, 2004, p. 80]

paradigm. The Design Science research cycle consists of two processes that *(1) build* and *(2) evaluate* the different types of artifacts that are part of an information system. Design science research uses the theories built by behavioral science and generates distinct artifacts that can be used in later project phases to implement concrete information systems.

> IT artifacts are broadly defined as constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices), and instantiations (implemented and prototype systems).
> [Hevner, 2004, p. 77]

In the case of this thesis the underlaying theory is the theory on organizational resilience. It provides *semantic definitions, interrelations, dependencies, and further theory-elements* that are elicited and modeled as artifacts in the Design Science research process. The interrelations between Design Science in Information System Research, its environment and the related knowledge base are visualized in Figure 2.6.

Design Science research must be seen as iterative process consisting of *(1) the generation and design of models* and *(2) the test of models against requirements* in an alternating cycle. The core question of Design Science is "What utility does the new artifact provide?"', [Hevner, 2004, p. 91]. This shows that *the aim is not to predict human or organizational behavior, but to provide models that are of use for people and organizations.* The evaluation of this use can on the one side be done be evaluating the developed models against business needs, depicted in Figure 2.6, or by implementing models and evaluating their utility in daily business life.

2.3.2 The Application of the Design Science Research Process

The research process for the thesis follows the clear concept Design Science in Information System Research. Due to the limited scope of a thesis and the complexity of the models that will be developed, the evaluation of the models will be conducted as theoretical evaluation of fulfillment of business needs. In the concrete case of this thesis, the business needs for risk and resilience management base on empirical research [Kaplan and Mikes, 2012, 2013; McManus, 2008; Stephenson, 2010; Weick, 1993, 1995, 2001; Weick et al., 2008] and the research cycle includes the required theoretical foundations [Argyris, 1977; Arrow, 1964; Beer, 1972; Foerster, 2003; Schwaiger, 2012; Wiener, 1963]. Founding on the business needs and the research process-flow, that will be illustrated in the subsequent paragraphs and on Figure 2.7, the logical line of argument required for scientific reasoning in Design Science are completely fulfilled. The implementation of the developed models and the evaluation within an enterprise might be part of future research projects.

The Research Process-Flow

1. *Analysis of risk management literature* with a focus on enterprise risk management frameworks. The analysis provides an overview over the development of the risk management domain within the last two decades. An elaboration of *definitions for risk, risk management and enterprise risk management* is conducted. An overview over the most influential and diffused risk management frameworks is presented, what serves as an information-basis for the decision on which risk management standard will be modeled in detail in Chapter 5. In this chapter research question one (RQ1) will be answered.

2. *Analysis of resilience management literature* including research with empirical evidence as well as best practice models and standards. Elaboration of a general *definition of organizational resilience* and evaluation of existing organizational resilience management standards as basis for the choice of the best applicable standard for the cybernetic modeling in Chapter 5. In this chapter research question two (RQ2) will be answered.

3. *Analysis* OF the ISO 31000 Risk Management Standard, *development of a Cybernetic Risk Management Framework* and visualization as hierarchical Management Activity Diagram basing an Schwaiger's Generic Cybernetic Management Framework [2012]. Elicitation of common elements of resilience including activities, information, information flow and resources for the *development of an risk management ontology* as UML Class Diagram [OMG, 2011]. In this section the research question three (RQ3) will be answered.

4. *Analysis* OF the ASIS SPC.1-2009 Organizational Resilience Management Standard and *development of a Cybernetic Resilience Management Framework*, again, visualized as Management Activity Diagram basing on Schwaiger's Generic Cybernetic Management Framework. Examination and determination of core resilience management activities, interactions, flow of information-entities and control elements on different cybernetic levels of an organization. *Development of a resilience management ontology* using UML Activity Diagrams [OMG, 2011]. In this section the research question four (RQ4) will be answered.

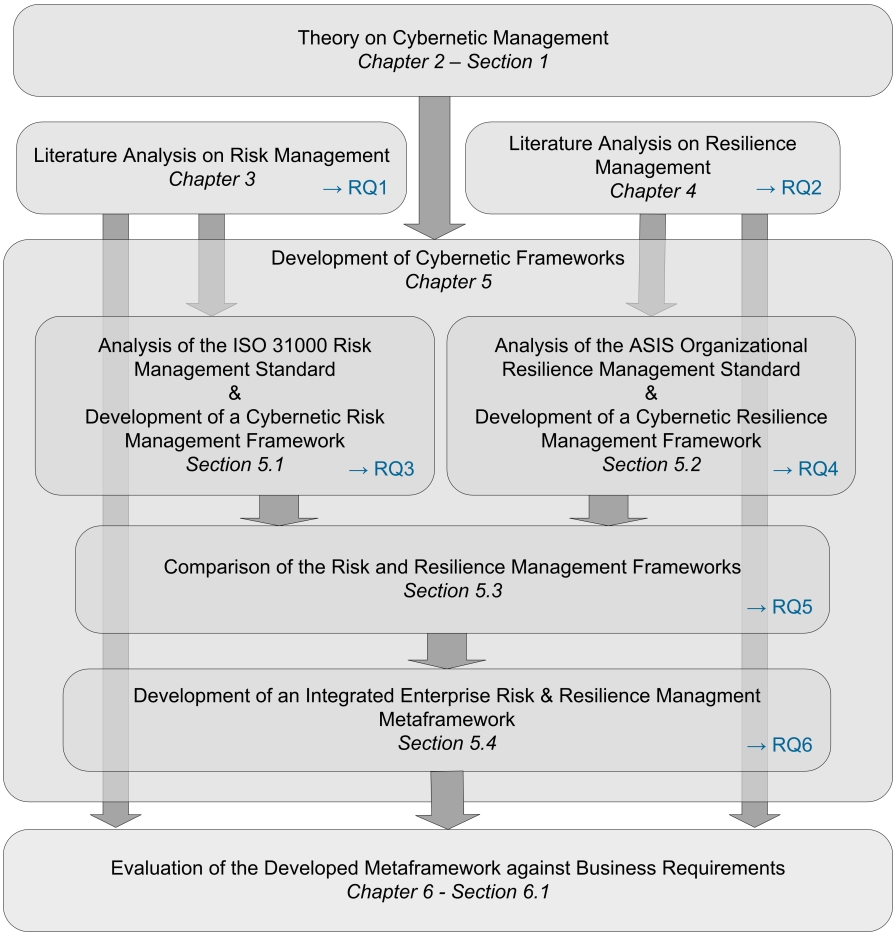

Figure 2.7: Methodological Approach for the Thesis

5. *Comparison* and, if necessary, *integration of the two developed cybernetic frameworks*. Comparison of the incorporated management activities, information elements and structures, as well as information flow. If these elements of the cybernetic frameworks differ to a relevant extent, an evaluation, whether an integration is possible, and an integration of the frameworks follows. In this section research question five (RQ5) will be answered.

6. *Development of an Integrated Cybernetic Enterprise Risk and Resilience Management Meta-Framework.* Theoretical integration-attempt of Schwaiger's Generic Cybernetic Management Framework (CMF) [2012] and Schwaninger's General Model of Systemic Control (MSC)[2001b, p. 141]. If the integration is feasible, the new integrated model will be applied to integrated eterprise risk and resilience management to provide a neta-framework for planning and control of risk and resilience management on all organizational levels and entities of an enterprise. In this section research question six (RQ6) will be answered from a "planning and control view".

7. *Evaluation of the developed management frameworks* against the empirical evidence on resilient organizations (elaborated in the preceding literature analysis) and assessment of the degree of coverage of resilience attributes and indicators by the new developed frameworks. The Cybernetic Management Frameworks base on the paradigm of "control in the large and control in the small". It shall be evaluated, whether different approaches and paradigms of managing risks and resilience exist, and whether they can be integrated into the framework itself, or whether they can be used for the implementation of the framework in an organization. In this section empirical evidence and further scientific paradigms will be added to answer Research Question Six (RQ6).

These seven process-steps fully implement the prescribed research process of the Design Science methodology. The scientific rigor was explained in the section above and the justification for the choice of Design Science as research methodology is explained in the section below.

2.3.3 Justification of the Methodology

The core methodology of the thesis is the *Design Science* approach. Its application includes the *Cybernetics* or *General Systems Methodology* als theoretical foundation and *existing empirical research on resilience indicators* as core business needs for resilience management.

The choice of the General Systems Methodology as theoretical fundament was met due to the fact that the complex business domain of risk and resilience management still lacks a main steering model that can be used by managers to implement a rigorous management system. According to the World Economic Forum (WEF), globalized economic systems are too complex for predicting risks with mathematical calculations [2013, p. 37]. The WEF arguments that *systems thinking, or cybernetics*, provides a useful foundation for assessing resilience, as the systemic approach considers many relevant elements and attributes of analyzed systems like the robustness, redundancy, resourcefulness as well as ways of response and recovery.

Ashby, co-developer of the theory on cybernetics, explained in the *Contant-Ashby Theorem* that:

> Every good regulator of a system must be a model of that system. [...] In other words, the results of a management process cannot be better than the model on which it is based, except by chance.
> [Schwaninger, 2001a, p. 1210]

This means that models for risk and resilience management must not be reduced in a too simple manner, for example by only focusing on sole mathematical theory. In contrast, a comprehensive model of reality, has to be used to seriously deal with complex problems in enterprise risk and resilience management. The application of Design Science meets these requirements very well. In the case of this thesis it utilizes the semantics, definition and theory-elements of the General Systems Theory as scientific foundation and models the risk and resilience management system in the sense of Ashby's theorem.

The advantage of the Design Science methodology is that the resulting model can first be used as meta-steering model for risk and resilience managers and second as basic design of risk

and resilience management information system. van Aken and Romm [2009] promote the use of the Design Science methodology in organizational science. The argue that Design Science has the potential to "mitigate the relevance problem of organization and management studies by producing knowledge that is geared toward designing solutions for field problems", [2009, p. 10]. This argumentation underlines that the Design Science method might bring usable solutions into the fuzzy field of organizational risk and resilience management.

CHAPTER 3

Risk Management

" The major difference between a thing that might go wrong and a thing that cannot possibly go wrong, is that when a thing that cannot possibly go wrong goes wrong, it usually turns out to be impossible to get at or repair it. "

[Douglas Adams, 1952 - 2001.]

Contents

3.1 Risk Management Models **19**
3.2 Current Trends in Risk Management **24**
3.3 Prevalent Problems in Enterprise Risk Management **27**
3.4 Key Findings **29**

Abstract The aim of this chapter is to provide an overview over relevant risk management standards, current research trends and problems concerning the actual implementation of risk management as part of enterprise management. In the subsequent elaboration the risk management standards that fit best to the cybernetic management approach are presented.

3.1 Risk Management Models

In this section well established risk management standards are presented in order to provide a theoretical foundation for the elaboration of a cybernetic risk management framework in Section 5.1. The selection of relevant standards bases on the nearness to the cybernetic management concept [Schwaiger, 2012]. This means that the standard has to support the process-view on risk management, the achievement of organizational objectives through proactive decision-processes that directly address uncertainties and the continual improvement of the implemented standard. The Risk Management Society (RIMS) published an encompassing report that compares modern

risk management standards [2011]. The analysis of this report showed that the most suitable and widely used risk management standards are the COSO Enterprise Risk Management Framework and the ISO 31000 Risk Management Standard. Therefore the core elements, processes and principles of both standards will be outlined.

3.1.1 The COSO Enterprise Risk Management Framework

The COSO Enterprise Risk Management Framework [2004] is the first risk management standard that takes the concept of proactive risk management to the enterprise level. All risk management activities can be planned, implemented and controlled in different organizational entities like subsidiaries, business units or divisions. In the COSO framework risk management is defined in the following way:

> Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.
> [COSO, 2004, p. 2]

To make enterprise risk management activities controllable, the objectives of different entities are divided into four distinct but overlapping categories. This means that one objective can be part of different categories and addresses different needs of an enterprise entity [COSO, 2004, p.2]:

- *Strategic objectives* are high-level goals, aligned with the entity-mission.
- *Operation objectives* shall ensure the effective and efficient use of the entity ressources.
- *Reporting goals* seize the reliability of the entity reporting.
- *Compliance goals* are used for assuring the compliance with laws and regulations that are applicable to the entity.

The accurate implementation and use of the enterprise risk management framework provides assurance for the achievement of reporting and compliance objectives. The achievement of strategic and operations objectives are "subject to external events" [COSO, 2004, p. 3] and are therefore not within the entity's sole control. Nevertheless, enterprise risk management can inform the management in time on the extend of achievement and probability of achievement of certain objectives.

The core components that make up the enterprise risk management framework, besides the objective and entity-types, are according to COSO [2004, p. 3–4]:

- The *internal environment* includes the tone of an organization, the risk management philosophy, risk appetite as well as ethical values and integrity.

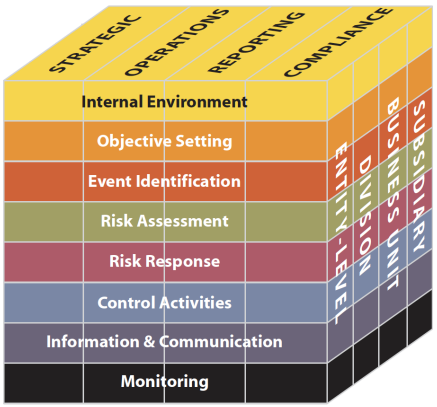

Figure 3.1: The COSO-Cube

Source: [COSO, 2004, p. 5]

- The *objective setting* means that objectives must be set before risk-associated events can be identified and that objectives must support the entity's mission as well as risk appetite.
- The *risk assessment* includes the analysis of risks, their likelihood and potential impact as a basis for the later determination of appropriate risk response actions.
- The *risk response* includes avoiding, accepting, reducing or sharing risk.
- The *control activities* ensure that risk responses are carried out in an effective way.
- *Information and communication* includes the identification, capturing and sharing of information so that people can carry out their risk management responsibilities.
- The *monitoring* includes the observation and control of the whole enterprise risk management system.

The enterprise risk management can only be effective if all "eight components are present and functioning effectively", [COSO, 2004, p. 5]. The fact that the achievement of strategic and operations objectives depends on the external environment is not the only limitation to the framework. A further one is the possible deficiency of human judgment in decision making [COSO, 2004, p. 5]. This aspect of psychological effects on persons' decision-making, as described in Kahnemann [2012], is not part of risk management standards and might be added by the concept of resilience management in later chapters.

The eight risk management activities and the four types of objectives can be applied to any organizational level of an enterprise: to the *subsidiary*, *business unit*, *division* and *entity level*. This shows that the COSO standard is explicitly designed for enterprise-wide risk management.

Since the publication of the COSO ERM standard, further work on the concept of internal control was conducted and COSO revealed a new framework called *Internal Control - Integrated Framework* [2013] and returned therewith to the original idea of COSO: internal control

including risk management to some extend. However, the Enterprise Risks Management - Integrated Framework COSO [2004] should not be replaced. In contrary, the concept of enterprise risk management is a broader concept that includes internal control as integral part, but focuses stronger on the broad approach of managing risks [COSO, 2011, p. 149]. So, the COSO ERM standard has lost none of its relevance within the last decade.

3.1.2 The ISO 31000 Risk Management Standard

The International Standardization Institution (ISO) introduced a new norm on risk management, called the ISO 31000:2009 Risk Management Standard [2009], and provided, besides the older COSO and FERMA standard[1] [2002], a new generic process oriented approach for managing risks.

A risk management framework is a systematic and transparent approach that has several goals. An excerpt of the most relevant goals and corresponding principles of the framework [ISO, 2009, p. V], for further analysis in Chapter 5, is presented in Table 3.1.

Goal	**Corresponding Principle**
Increasing the likelihood of achieving business goals.	Risk management creates value in all business and management areas.
Increasing the awareness of the need to identify and treat risk through the whole organization.	Risk management explicitly adresses uncertainty.
Improving governance and control.	Risk management is tailored and aligned with the organization's external and internal context and risk profile.
Improving reporting.	Risk management is based on the best available information (historical data, experience, stakeholder feedback, observation, forecasts and expert judgement).
Improving stakeholder trust.	Risk management is transparent and inclusive.
Establishing a reliable basis for decision making and planing.	Risk management is part of decision making.
	Risk management is transparent and inclusive. Stakeholders are involved and their views are taken into account in determining risk criteria.
Improving organizational learning.	Risk management takes human and cultural factors into account.
	Risk management facilitates continual improvement of the organization (to improve risk management maturity).
Improving organizational resilience.	Risk management is dynamic, iterative and responsive to change and facilitates the continual improvement of the organization.
Minimizing losses.	Risk Management protects values.
Encouraging proactive management.	Risk management is an integral part of all organizational processes

[1] The *FERMA Risk Management Standard* was the first generic and broadly used risk management standard that was publish by the Federation of European Risk Management Associations [2002].

Goal	Corresponding Principle
Effectively allocating and using resources for risk treatment.	Risk management is transparent.
Improving operational effectiveness and efficiency.	Risk management is systematic, structured and timely.
Improving loss prevention and incident management.	Risk management creates and protects value.
Improving the identification of opportunities (positive risk) and threats (negative risks).	Risk management explicitly adresses uncertainty.
Comply with regulatory requirements.	

Table 3.1: Goals and Principles of the ISO 31000 Risk Management Standard

Basing on these principles and goals, ISO defines risk in a broad way: “internal and external factors and influences that make it uncertain whether they [organizations] will achieve their objectives”, [2009, p. v] or as positive or negative “effect of uncertainty on objectives” [2009, p. 1]. According to ISO 31000, all activities of an organization involve risk management, the “coordinated activities to direct and control an organization with regard to risk”, [2009, p. 2]. This shows that the ISO standards must be, similar as the COSO ERM framework, applicable to all organizational levels of enterprises.

ISO 31000 consists of a set of components that build the foundation for planning, introducing, monitoring, reviewing and continuously improving risk management in an organization [2009, p. 2], as illustrated on Figure 3.2.

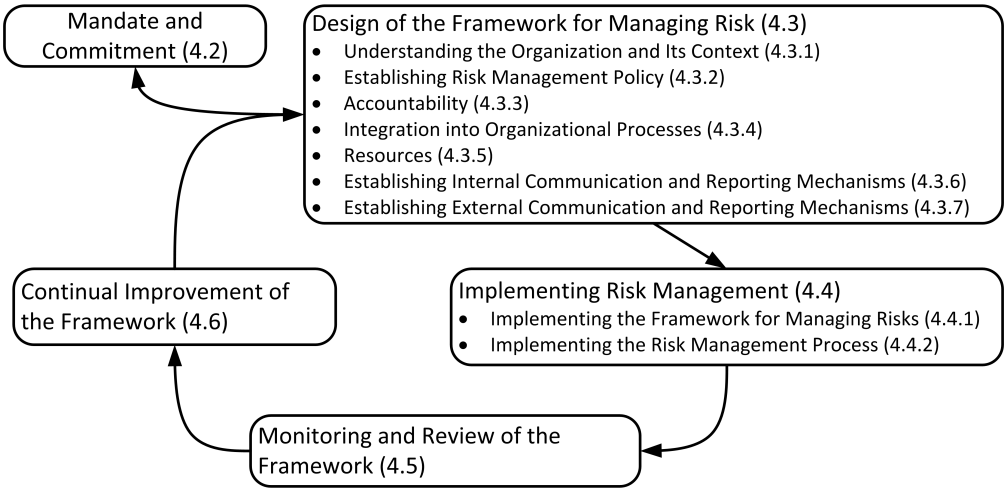

Figure 3.2: The ISO 31000 Risk Management Components

In Accordance with ISO [2009, p. 9]

When the risk management system has been set up in an organization, the core risk management process can be conducted in a recursive manner, as shown on Figure 3.3.

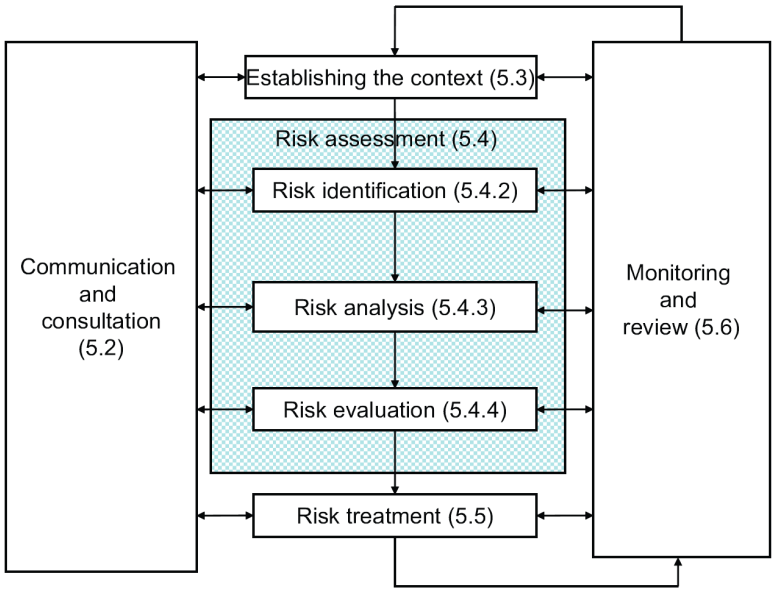

Figure 3.3: The ISO 31000 Risk Management Processes

Source: [ISO, 2009, p. 14]

The implementation of the ISO 31000 Risk Management Standard is, in a similar way as COSO, not restricted to a specific domain. Rather, it can be applied to any domain or industry [Gjerdrum and Peter, 2011], so the main advantage is that who ever comprehends the generic model, can apply it to a whole enterprise, community or any other organization.

3.2 Current Trends in Risk Management

Current research results show that the successful implementation of a risk management standard strongly depends on the sensible mix of risk management methods and the way an appropriate risk management culture is established. Considerations in this directions are elaborated below.

3.2.1 A Contingency Theory of Enterprise Risk Management

Kaplan and Mikes reveal a common problem of common risk management frameworks [2012, p. 51] and portray enterprise risk management as an evolving discipline [2013, p. 3], at the same time. They conducted a ten-year research project including 250 interviews with chief risk officers and three case studies on ERM in high reliability organizations. Basing on the results of this project they express their concern that “risk management is too often treated as a compliance issue”, [2012, p. 51] and the fact that this paradigm of risk management is neither suitable for reducing the likelihood nor for reducing the impact of real disasters like Black-Swan events [Taleb, 2013]. Kaplan and Mikes argue that the prevailing duty of risk management research is to develop new paradigms or models that help to identify and prepare for non-preventable ex-

ternal risks. In order to facilitate the emergence of new risk management models they introduce three categories of risks that allow the differentiation between types of risks and corresponding paradigms of treatment.

1. *Preventable risks* are controllable risks that arise within an organization and can be avoided [Kaplan and Mikes, 2012, p. 51]. According to Kaplan and Mikes, this category of risks can be managed best by *monitoring and control* as well as operational processes that guide behavior and decisions of employees towards desired norms.

2. *Strategy risks* arise for enterprises from employing strategies that generate superior returns. Kaplan and Mikes report that this kind of risks can not be managed by "rule based control models", [2012, p. 52]. However, they do not propose to choose less risky strategies as this type of risks is, at the hear of economic theory, not undesirable. In contrary, they argue for the necessity of a risk management system that enables managers *to reduce the probability of risks and to increase the capability to manage the risks if they realize, at the same time.*. If enterprises have employed such risk management systems, they can choose more risky strategies providing higher rewards. This type of risk management system comprises a direct competitive advantage as it can be seen as a non-material resource that is difficult for competitors to imitate [Porter, 2008]. Methods for the management of strategic risks are *interactive discussions* that include maps of likelihood and impact, key risk indicator scorecards and resource allocation to mitigate severe risk events [Kaplan and Mikes, 2012, p. 57].

3. *External risks* "arise from events outside the company and are beyond its influence or control", [Kaplan and Mikes, 2012, p. 52]. This kind of risk includes natural, political, economic and socioeconomic disasters. Kaplan and Mikes explain that risk managers are unable to plausibly asses the likelihood of such complex external events [2013, p. 12]. Especially global systemic risks that relate with the postmodern way of life and trade [Jameson, 1991] fall in this category [WEF, 2012, 2013]. The management of external risks requires *"open and explicit risk discussions"*, [Kaplan and Mikes, 2012, p. 52]. Methods for managing uncontrollable external risks focus on "envisioning risks through tail-risk assessments and stress testing [...] scenario planing [...] war-gaming", [Kaplan and Mikes, 2012, p. 57].

Kaplan and Mikes found out that ERM research has been treated as uni-dimensional in meaning of "either you have adopted ERM or not" [2013, p. 26]. In order to be grounded in reality they stipulate an "ERP-mix", [Mikes, 2009 qtd. in Kaplan and Mikes, 2013, p. 26] including (a) processes for identification, assessment and rolling-up risks, (b) a fitting frequency of risk roll-ups, (c) risk tools, (d) a linkage between risk management and other control and (e) the central role of the chief risk officer. As result of these research findings they developed a contigency framework for enterprise risk management and advocate firstly the "unpacking of the ERM mix into its fundamental building blocks", [p. 29] and secondly highlight the distinction of the three identified categories of risks, so that separate risk management processes can address the different risk types.

3.2.2 Models of Risk Culture

The Institute for Risk Management (IRM) adduces several case studies that show that *deficiencies in leadership, competency, communications and culture* were the causes for severe disasters in the recent past [IRM, 2012]. As consequence the IRM developed a risk culture aspects model to makes responsible risk managers aware of central aspect in cultural change management projects that should lead to better results in the management of external risks, which are the core problem of current risk management approaches [Kaplan and Mikes, 2012; Taleb, 2013; WEF, 2012, 2013]. The *Risk Culture Aspects Model* is depicted in Figure 3.4.

Figure 3.4: The Risk Culture Aspects Model

Source: [IRM, 2012, p. 14]

Mikes introduces the notion of *calculative cultures* "capturing senior managerial attitudes towards the use and limitations of highly analytical calculative practices in an organization", [2009, p. 21]. She distinguishes between calculative idealism and calculative pragmatism that Power had introduced [Power qtd. in 2009, pp. 21-22]: In cultures of *calculative idealism* the focus lies on managing risk 'by the numbers', what comprises the underlying assumption of quantitative enthusiast managers that risk measures are capable of reflecting economic reality. Organizations with a culture of *calculative pragmatism* see risk metrics as trend indicators which can be overruled by senior managers on the basis of experience and expert judgement.

In relation with these two risk cultures, Mikes presents four ideal types of enterprise risk management: (1) risk silo management, (2) integrated risk management, (3) risk-based management and (4) holistic risk management [2009, p. 26]:

1. *Risk silo management* has its origin in international regulations of bank capital adequacy. The management focuses is on risk quantification and control of risk silos using concepts like *value-at-risk* and *credit rating models*.

2. *Integrated risk management* roots in the expectations of rating agencies concerning bank

capital adequacy.[2] The used methodology is *risk aggregation* and risk limit setting on economic capital.

3. *Risk-based management* is coined by the rise of the shareholder value imperative and governed by quantitative enthusiasm. The goal is to establish a *risk-based performance measurement* by combining risk management with performance measures. Used methods are risk-adjusted return on capital, shareholder value added and portfolio risk management.

4. *Holistic risk management* arose with the growing impact of risk-based internal control due to the Sarbanes Oxley Act[3] and 8^{th} Directive of the European Parliament[4] and is governed by quantitative scepticism. It *includes the management of non-quantifiable risks* into the risk management framework, what provides senior managers with a strategic view on risks and makes the whole ERM an adaptive learning machine. Techniques of holistic risk management are *scenario analysis, sensitivity analyses, control self assessment* and *risk reviews*.

Mikes admits that it is still unclear to which extent the different ERM models are mutually exclusive. She raises a new question that has to be answered: "Do they represent a divergence in the risk management world, or are they different stages in the evolution of risk management?", [2009, p. 37]. Maybe the later analysis and development of a cybernetic ERM framework in Part 5 will contribute some aspects to the answer of this question.

In similar ways as Kaplan and Mikes describe the necessity of taking strategy risks for staying competitive in any field of business. Ashby et al. introduce the tentative conceptual model of risk culture visualized on Figure 3.5. The strategic positioning concerning risks is a major element of business success, as risk is a fundamental part of all kind of business [Ashby et al., 2012, p. 10]. Firms have to take risks. If they try to minimize risks they raise the risk of bankruptcy.

3.3 Prevalent Problems in Enterprise Risk Management

Kaplan and Mikes explain that enterprise risk management is too often segregated into functional silos and rooted in the compliance field [2013, p. 11]. They elaborate, by the examples of the Global Financial crisis, the BP Deep Horizon's explosion and the problems during the

[2]The Basel Committee on Banking Supervision published the *International Convergence of Capital Measurement and Capital Standards* [2006], often being referred to as *Based II*. This standard provides rules and criteria for the internationalization and convergence of capital measurement.The intention was to regulate how much capital international banks need to put aside to decrease different types of financial and operational risks on the banking business. In 2010 the Committee published *Basel III: A global regulatory framework for more resilient banks and banking systems* [2010] and continued to route towards resilience they started with Basel II.

[3]The 107^{th} Congress of the United States of America passed the Public Law 107-204, also called *Sarbanes-Oxley Act of 2002*. One main target of the Sarbanes-Oxley Act, which is related to the elaborations on risk and control systems above, was to force large enterprises to implement and maintain an effective internal control system [US-Congress, 2002].

[4]The European Parliament and the Council of the European Union passed the *Directive 2006/43/EC* [2006]. This directive forced the member states of the European Union to enact laws that impose the necessity of effective and efficient internal control systems on large companies.

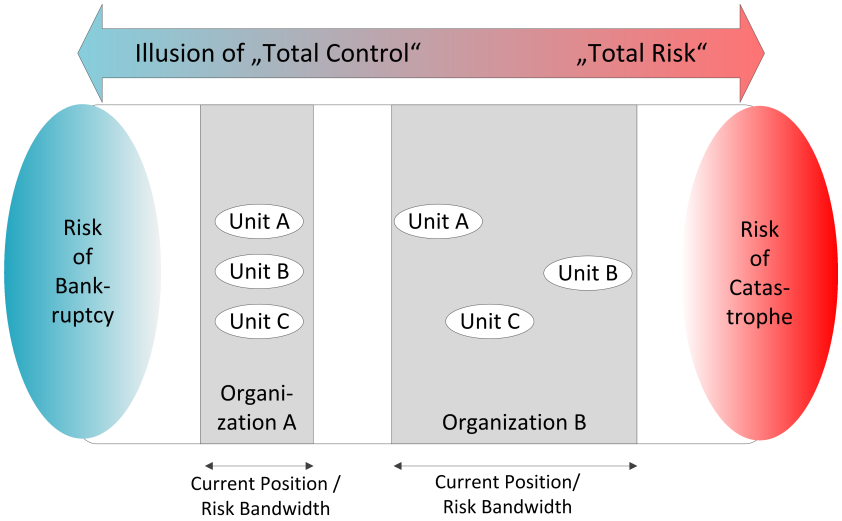

Figure 3.5: Tentative Conceptual Model of Risk Culture

In Accordance with Ashby et al. [2012, p. 10].

development of the new Boeing 787 Dreamliner, that these approaches do not help to avoid real disasters. According to them, the prevailing paradigm of *control in the large* and *control in the small*, developed by Arrow [1964], appears to be an inappropriate approach for dealing with external hazards.

In a similar way, Power describes that in spite of the critics on risk management frameworks and legal regulations, like Sarbanes Oxley and Basel II, a change of the risk management narrative has not happened up to now. ERM has become lost in the "procedural detail of organization-specific internal control, compliance and accounting systems", [Power, 2009, p. 854].

Even though, many firms use risk management frameworks, only 40% of them use risk management for all decisions [G31000, 2012] while "all activities of an organization involve risk", [COSO, 2004, p. V] and involve risk management [ISO, 2009, p. 1]. The same problem adduce Price Waterhouse Coopers [2004] by explaining that many CEOs see ERM as an external accountability and not as integral part of management activities. Therefore, a seamless integration into of risk management into enterprise management is necessary.

Additional to the depicted organizational problems in ERM, there exist employees' strong biases that prevent them from thinking about risks until they it is too late [Kaplan and Mikes, 2012, p. 51] (compare [Kahnemann, 2012; Kaplan and Mikes, 2013; Taleb, 2013]).

In the last years, risk appetite focused more on capital than on actual human behavior what is, according to Power, an important source of the intellectual failure within ERM models, "that should be addressed by regulators, senior management and boards", [2009, p. 854]. He claims that a stronger focus on risk appetite as a process could help represent and materialize the "complex ecology of operational values and shifting ethical limits", [2009, p. 854].

3.4 Key Findings

KEY FINDINGS

- Risk can have positive or negative impact on the achievement of business objectives.
- The management of risk includes the analysis and treatment of risks on all organizational levels and should be part of everyday management during all kinds of decisions.
- Risk is a fundamental part of all business. Firms have to take risks. If they try to minimize risks they raise the risk of bankruptcy.
- There exist distinct types of risks like internal, external, financial, operational and strategy risks that require different methods of identification and treatment.
  (This typology is not all-inclusive, but includes the view of current research trends.)
- ISO 31000 and COSO II are the most diffused and advanced enterprise risk management standards.
- The way ISO 31000 and COSO II are commonly implemented in enterprises often lacks methods to prepare for unpredictable external risks, called Black Swans.
- The successful implementation of ERM systems is always intertwined with cultural development.
- Current challenges for risk management are to develop new risk management models using different economic and scientific paradigms that can help to deal with systemic external risks, called black swans, that can not by influenced by the organization itself. The concept of resilience management might be one approach to enlarge enterprise risk management in a way that makes organizations more likely to survive these black swans.

ANSWER TO RESEARCH QUESTION 1

1.1 How does the scientific and industrial management community define risk?

- *Risk is an internal or external factor that has a potential impact on the reaching of objectives, where the effect of uncertainty can be positive or negative (adopted from ISO [2009]).*

1.2 How does the scientific and industrial management community define risk management?

- *Risk management is the conduct and coordination of activities to direct and control an organization with regard to risk (adopted from ISO [2009]).*

1.3 How does the scientific and industrial management community define enterprise risk management ?

- *Enterprise risk management is a process across all management and business levels of an organization, designed to identify and manage potential events that may affect the entities of the organization in order to achieve its objectives (adopted from COSO [2004]).*

CHAPTER 4

Resilience Management

" For many companies the future is less unknowable than it is unthinkable, less inscrutable than unpalatable. "

[Gary Hamel, born 1954.]

Contents

4.1 Organizational Resilience **31**
4.2 Resilience Management Models **38**
4.3 Key Findings **43**

Abstract This chapter includes an introduction into empirical research results on organizational resilience as well as an overview over resilience management models and the related scientific paradigms that could possibly be used for the development of an integrated risk and resilience management model in Chapter 5.

4.1 Organizational Resilience

Organizational resilience is the capability of an organization[1] to recover from any kind of negative impact or crisis. Sutcliffe and Vogus, who conducted empirical and theoretical research on organizational resilience for several years, define resilience as *"the maintenance of positive adjustment under challenging conditions such that the organization emerges from those conditions strengthened and more resourceful"*, [2007, p. 3418] where the conditions can be exogenous shocks and ongoing strain. According to Sutcliffe and Vogus, resilience requires the presence of

[1] Westley defines an organization as "a series of interlocking routines, habituated action patterns that bring the same people together around the same activities in the same time and places", [1990 qtd. in Weick, 1993, p. 632].

resources that can be activated and combined in challenging situations. Resilient organizations are aware of the fact that their models of risks as well as their countermeasures are incomplete and need regular update [2007, p. 3419]. They clarify that the idea of margin, for example in financial or human resources, is crucial for resilience [2007, pp. 3420, 3421]. They adduce that resilient organizations have a more nuanced picture of ongoing operations than other organizations and invest more targeted and timely in order to defuse upcoming risks.

According to Sutcliffe and Vogus, there exist three types of resilience: (1) resilience at the individual level, (2) resilience at the group level, and (3) resilience at the organizational level [2003, pp. 99–106]. At all three levels two elements are responsible for the degree of resilience: (a) sufficient resources to build and enhance competence and (b) the mobilization mastery of motivation systems to foster growth and efficacy. At the organizational resilience level these capabilities include the following activities [Sutcliffe and Vogus, 2003, p. 106]:

a i Increase the amount and quality of resources through improvisation and recombination.

ii Develop and maintain conceptual slack.

b i Develop organizational structures[2] that allow flexible rearranging and transferring of expertise and resources (e.g. ad hoc problem solving networks, social capital).

ii Enhance capabilities to quickly process feedback.

If the resources and the mobilization mastery of motivation systems is available at all levels of resilience, a resilient response to crises can be made more probable. At the beginning of or during a crisis, usual organizations initiate very rigid responses [Sutcliffe and Vogus, 2003, p. 106] including the narrowing of information processing, the tightening of control and the conservation of resources, what often leads to a negative adjustment. In resilient organizations quite the opposite happens: information processing is broadened, control is loosened and slack capabilities are utilized in a senseful way, as visualized on Figure 4.1. At the first sight this resilient response seems to contradict the common culture of planning and control in enterprise risk management.

To understand, how a resilient approach can be introduced in organizations, further subelements and subsystems or resilient crisis responses have to be understood. Therefore, the following pages provide an introduction into the empirical research on elements and indicators of organizational resilience.

4.1.1 The Emergence of Resilience

A central work that initiated the research process on organizational resilience was Weick's analysis of the Mann Gulch Fire Disaster [1993]. He tried to find out why organizations unravel and how organizations can be made more resilient. The main results of Weick's research can be found in the following paragraphs.

[2]Mintzberg defines five criteria for a simple organizational structure: "Coordination by direct supervision, strategy planned at the top, litte formalized behavior, organic structure, and the person in charge tending to formulate plans intuitively, meaning that the plans are generally a direct extension of his own personality", [1983 qtd. in Weick, 1993, pp. 632-633].

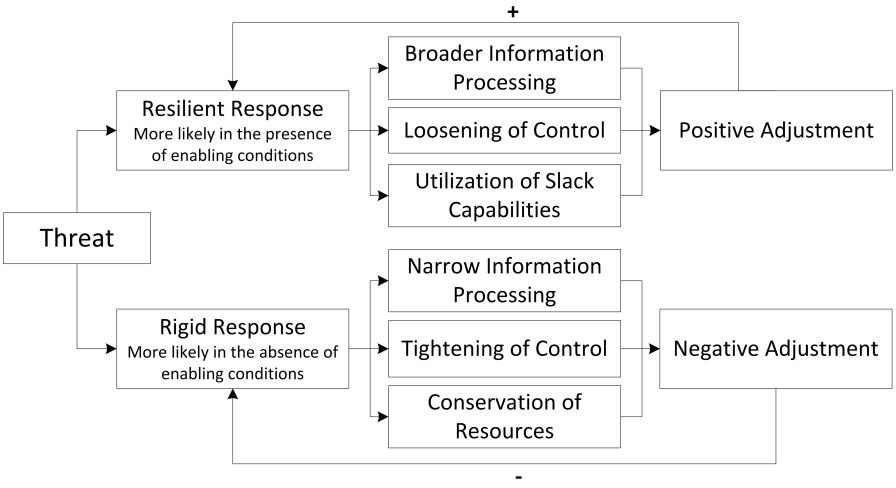

Figure 4.1: Resilient and Rigid Crisis Response

In accordance with Sutcliffe and Vogus [2003, p. 107].

The Loss of Meaning and Structure during Disasters

Weick revealed that during a crisis members of organizations are struck by the feeling that "the universe is no longer rational", [1993, p. 663]. Weick defines such happening as *cosmology episode* or a *vu jàdé*, the opposite of a déjà vu, a situation one has never seen before [1993, p. 634]. According to him, people *loose (1) the sense of what is occurring, at the same time, with (2) the means to rebuild this sense*. Weick explains that the crisis of Mann Gulch arose by the simultaneous collapse of sensemaking and organizational structure. He analyzed the incident in detail, by scanning historical documents and by interviewing involved persons, in order to understand it and to become capable of preventing similar disasters in other organizations.

In order to regain the lost sense of what is occurring a process called *sensemaking*, a retrospective action of making sense of what happes, must occur [Weick, 1993, p. 635]. Weick states that people construct their reality by finding patterns of significant meaning in a situation. He clarifies that, in contrast to decision making what is about clear questions and strategic rationality, sensemaking is about vague questions, negotiated agreements and contextual rationality what bears the chance to reduce confusion [1993, p. 636].

A main cause for the Mann Gulch disaster was the *damage of the* only structure the firefighters had, the *role structure* what made the following question arises: "If I am no longer a firefighter, then who am I?", [Weick, 1993, p. 637]. Not only the sense of what was happening, but also the sense of who am I, what is my role, and what does the organizational structure look like, was missing. Bass made similar observations and asserts that groups that do no longer interact easily or do no longer have a useful structure that allows quick reactions, are prone to experience stress [Bass 1960 qtd. in Weick, 1993, p. 644]. Ranson, Hinings, and Greendwood [1980 qtd. in Weick, 1993, p. 644] define structure the following way:

> [Structure is] a complex medium of control which is continually produced and

> recreated in interaction an yet shapes that interactions: structures are constituted and constitutive of interpersonal cognitive processes, power dependencies, and contextual constraints.

Once structure and meaning is lost within an organization or group, one of both has to be rebuilt in order to stop the self-enforcing cycle of disorientation. When an organizational structure and the common meaning of the business entity is destroyed by a hazard, a new meaning has to be gained before the structure can be built up again. The description of the processes of regaining meaning is part of Weick's elaborations.

Regaining Meaning

According to Weick, the restructuring consists of two patterns: The first pattern called *shared provinces of meaning* is an informal structure or social construction consisting of interaction patterns that stabilize meaning by the creation of shared interpretation schemes [1993, p. 645]. The second pattern is called *structural frameworks of constraints* which are contextual constraints that embody dominant meanings: a framework of roles, rules, activities, and authority relations that reflects and enables shared meanings [1993, p. 645].

Meanings and frameworks are constituted in a mutual way as deviation-amplifying feedback loop [1993, pp. 654, 646]. Weick rationalizes that one way to prevent the amplification is to reverse the feedback loop (of less role structure leading to less meaning) and to create an inverse relation between meaning and structural framework (less meaning leads to more structure, and vice versa). The essential element to turn these negative feedback loops into positive ones is the change of attention between structural frameworks and provinces of meanings what leads us to two central hypotheses basing on Weick's elaborations [1993, p. 646]:

1. Missing structure requires meaning to increase structure.
2. Missing meaning requires structure to increase meaning.

He explains that both approaches constitute an "alternation between attention to frameworks and attention to meanings", [1993, p. 646]. In how far sensemaking is also part of the planning and control approach or can be integrated into the approach may come to light In Chapter 5.

Further Attributes of Resilient Organizations

Additionally to thy dynamic cycle between meanings and frameworks, Weick found four sources of organizational resilience: (1) improvisation and bricolage, (2) virtual role systems, (3) the attitude of wisdom, and (4) respectful interaction [1993, p. 683].

Weick shows that creativity or *(1) improvisation and bricolage* under pressure increases the chance to prevent disasters [Weick, 1993, p. 640]. It appears that one primary challenge for organizations under pressure is to balance the use of necessary rigorous planning on the one side and improvisation and creativity on the other side. One specific realization of improvisation can be the construction of a *(2) virtual role systems* during a crisis. If this happens inside the head of persons, an organization can still continue to function after the real role system has disappeared

to function in tangible activities. If employees are able to build such a virtual role system, it makes it easier for them to keep up or restart *(3) respectful interaction*, what again creates intersubjectivity [Wiley 1988 qtd. in Weick, 1993, p. 642]. Weick describes, that intersubjectivity is constituted by two characteristics: first, the interchange and synthesis of meanings between human beings and second, the transformation of subjects during the interaction so that a common subjectivity develops. Main elements of respectful interaction are trust, honesty, and self-respect and social support [Weick, 1993, p. 643]. This makes clear that lost meaning can only be rebuilt in a group by interaction, and interaction is easier if some group-members are able to construct a virtual role system. Regarding the respectful interaction, Weick refers to Ginenett's research on excellent crews. Ginenett explains the necessity of respectful interaction in a similar way constituted by four basic characteristics: "I need to talk to you; I listen to you; I need you to talk to me; or even I expect you to talk to me" [1993 qtd. in Weick, 1993, p. 650]. As a final element of resilience the *(4) attitude of wisdom*, defined as "an attitude taken by persons toward the beliefs, values, knowledge, information, abilities, and skills that are held, a tendency to doubt that these are necessarily true ore valid and to doubt that they are an exhaustive set of those things that could be known." [Meacham 1983 qtd. in Weick, 1993, p. 641], is a necessary competence of group-members that want to be able to build their own virtual role-system.

> Extreme confidence and extreme caution both can destroy what organizations most need in changing times, namely, curiosity, openness and complex sensing.
> [Weick, 1993, p. 641]

These insights into resilient organizations involve an apparent discrepancy between its constitutive elements: creativity versus planning, confidence versus doubt, and virtual role systems versus real organizational structure. To gain a deeper understanding and the chance to dissolve some antithesis, we take a closer look at the type of organization that is professionally occupied with the mastering of severe crises, namely high reliability organizations (HRO) like atomic plants or the aviation industry.

4.1.2 High Reliability Organizations as Prototypes of Resilience

While analyzing high reliability organizations (HRO) Weick et al. [2008] discovered a special mindset that is common to all HROs. He calls it *mindful awareness*. This type of awareness is constituted by five subelements: (1) precoccupation with failure, (2) reluctance to simplify interpretations, (3) sensitivity to operations, (4) commitment to resilience, and (5) undespecification of structures. The construction of mindfulness is visualized inf Figure 4.2.

> The language of a near miss, having the bubble, migrating decisions, conceptual slack, resilience, normal accidents, redundancy, variable disjunction, struggle for alertness, performance pressure, situational awareness, interactive complexity, and prideful wariness, describes how people organize around failures in ways that induce mindful awareness.
> [Weick et al., 2008, p. 62]

(1) Preoccupation with failure means that HROs preoccupy with incidents they seldom see [Weick et al., 2008, p. 39], called *Black Swan Events* [Taleb, 2013]. In order to enable proactive

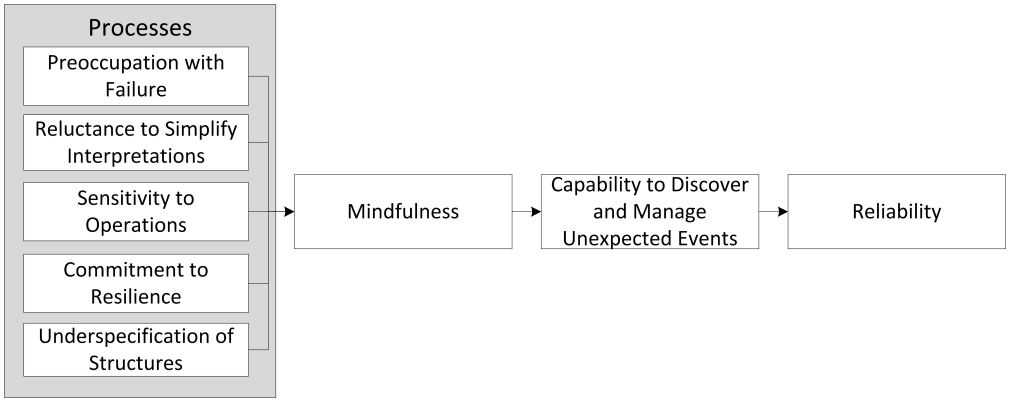

Figure 4.2: Processes for Mindfulness

In accordance with Weick et al. [2008].

learning by getting more data points they broaden the number and types of failures they pay attention to by analyzing so called near misses .[3] In contrast to most organizations, they do not only localize failure, but generalize it to prevent future hazards. They tend to remain fully informed as they "self-organize to encourage and reward the selfreporting of errors", [Rochlin 1994 qtd. in Weick et al., 2008, p. 40]. This elucidates that the respectful interaction, as described above, requires a special kind of reward system and organizational culture.

However, not all problems can be solved by preoccupation. Many situations in business life involve extreme complex situations. Members of usual organizations tend to simplify complex tasks in order to be able to cope with them in a reductionist manner. Weick describes these simplifications as *worldviews, frameworks, or mindsets* which "allow members to ignore data and keep going", [Weick et al., 2008, p. 41]. These simplification mechanisms result in so called basic assumptions within organizations which members of the organization get socialized with [2008, p. 42]. HROs in the opposite are *(2) reluctant to simplify interpretations* and cultivate requisite variety[4], to promote mindful awareness. They match the internal complexity of the organization with external complexity of the organizational environment.

> These efforts take such forms as diverse checks and balances embedded in a proliferation of committees and meetings, frequent adversarial reviews, selecting new employees with non-typical prior experience, frequent job rotation, and re-training. [Weick et al., 2008, p. 42]

HROs act on the belief that all humans are fallible, typical members of HROs operate very sceptic and get double-checked by another skeptic. This seems to be a more expedient mindset than the one of the dominant all-knowing manager. Weick even goes so far to define organizations as by what they ignore and by what can surprise them [2008, pp. 41, 43].

[3] *Near misses* are critical events that organizations "gets by, but only just" [Stephenson, 2010, p. 222].

[4] *Requisite variety* is the conceptual slack or divergence in perspectives among members of an organization over theoretical concepts and causal assumptions about technology or organizational processes [Schulman 1993b qtd. in Weick et al., 2008, p. 42].

This scepticism includes an surpassing *(3) sensitivity to operations*. Weick et al. explain it as the big chunk picture of operations in a current situation. A core task for organizations on the way to resilience is to keep the situational awareness during different types of pressure [2008, p. 44]. An indispensable prerequisite for this sensitivity is the sincere *(4) commitment to resilience*. While traditional organizations lean towards the anticipation of risks and planned defenses, HROs also bear the potential to cope with unanticipated impacts and learn to bounce back [Weick et al., 2008, p. 46]. Weick et al. describe that members of HROs self-organize ad-hoc networks that enable fast collection and exchange of cognitive knowledge in order to solve problems [2008, p. 47].

This commitment to resilience and the sensitivity to operations allows a certain *(5) under-specification of structures*. A rigid hierarchy can enlarge failures [Weick et al., 2008, pp. 48-49], so HROs allow decision making to shift with problems by subordinating a higher hierarchical rank to expertise and experience at the bottom of the hierarchy [p. 49]. This strategy can be successful when organizations have the cultural belief that the resources and capabilities for solutions lie within the organizational system.

According to Weick, the concept of organizational resilience still requires further empirical research to contribute to the scientific organization theory. Especially the "effectiveness, learning, meaningful levels of analysis, and requisite variety", [2008, p. 52] require shall be focused in future research projects.

4.1.3 The New Zealand Casestudies

McManus [2008] did multiple case studies to find out what the common components of resilience to all organizations in the New Zealand context are. A main research goal was to find out how organizations identify, assess and manage its vulnerability to high consequence/low probability events (compare Taleb [2013]). McManus conducted ten casestudies in different organizations and found *three attributes of resilience and 15 resilience indicators* which constitute the resilience attributes.The three resilience attributes are situation awareness, management of keystone vulnerabilities, and adaptive capacity. *Situation awareness* is the ability of an organization to stay aware of itself and its environment all the time and especially during different phases of crises [2008, p. 13]. *Keystone vulnerabilities* are the elements of an organization that encompass the highest probability to cause an huge negative impact on the whole organizational system [2008, p. 78]. *Adaptive capacity* includes all elements of organizational culture.[5] That allow the system to make decisions in an appropriate and timely way, either to use an opportunity or to cope with a crisis [2008, p. 87].

> Resilience is a function of an organizations's situation awareness, identification and management of keystone vulnerabilities and adaptive capacity in a complex, dynamic and interconnected environment.
> [McManus, 2008, p. 5]

[5] "*Culture* is an environment, a petri dish in which certain behavior and characteristics are allowed to flourish or not.", [John Harvie qtd. in IRM, 2012, p.7].

On the basis of McManus' research Stephenson set the goal to review the resilience indicators and to develop a resilience measurement tool. She conducted a research project including a web-based self-assessment for organizations, a pilot study including a factor analysis and semistructured interview within 34 organizations, as well as the final study including 68 organizations. The result of the her project was a simpler version of McManus' resilience model. In accordance with the research results she reduced the resilience attributes to *adaptive capacity* and *planning*. The primal 15 resilience indicators could be reduced to the number of 13 and can be found on Figure A.1 in the appendix.

4.2 Resilience Management Models

4.2.1 The ASIS Organizational Resilience Management Standard

The ASIS International SPC.1-2009 Organizational Resilience Standard is a management framework for anticipating, preventing and responding to disruptive events like emergencies, crises or disasters in order to increase the resilience of organizations and "to ensure the organizations's continued viability", [Blass, 2010, p. vii]. The standard explicitly adopts the *Plan-Do-Check-Act (PDCA)* process-management-model which includes clearly separated process-types for planning, implementation, operation, monitoring, review, maintenance and continual improvement. The process approach is illustrated on Figure 4.3. The standard is designed in a way that related frameworks of safety, information security and others can be integrated.

> *Organizational resilience management* [is constituted by] systematic and coordinated activities and practices through which an organization manages its operational risks, and the associated potential threats and impacts therein.
> [Blass, 2010, p. 47]

ASIS defines requirements for an organizational resilience management system that enable any organization to "develop and implement policies, objectives, and programs", [Blass, 2010, p. 1] that take the local and business-related legal and other requirements of organizations into account. The generic requirements provided can be incorporated in any type of organizational resilience management system as it provides "elements required to integrate management, technology, facilities, processes, and people into the resilience culture, risk management, and organizational resilience management system", [Blass, 2010, p. 1] . Starting with these requirements the organization derives the *critical assets* that have to be protected.

The requirements of the planning phase that every organization has to implement itself include the *scope of the organizational resilience management system (4.1.1)*, the *organizational resilience management policy (4.2)*, processes for *risk assessment and impact analysis (4.3.1)* and for the *identification of legal and other requirements (4.3.2)*. Further requirements are *objectives, targets, and programs (4.3.3)* to *avoid, prevent, deter, mitigate, respond to, and recover from disruptive incidents* [Blass, 2010, p. 8].

The evaluation phase includes ongoing measurement through performance metrics, evaluation of compliance, system testing and management reviews. The ASIS Organizational Resilience Management Standard is designed for continual improvement. Therefore, the evaluation

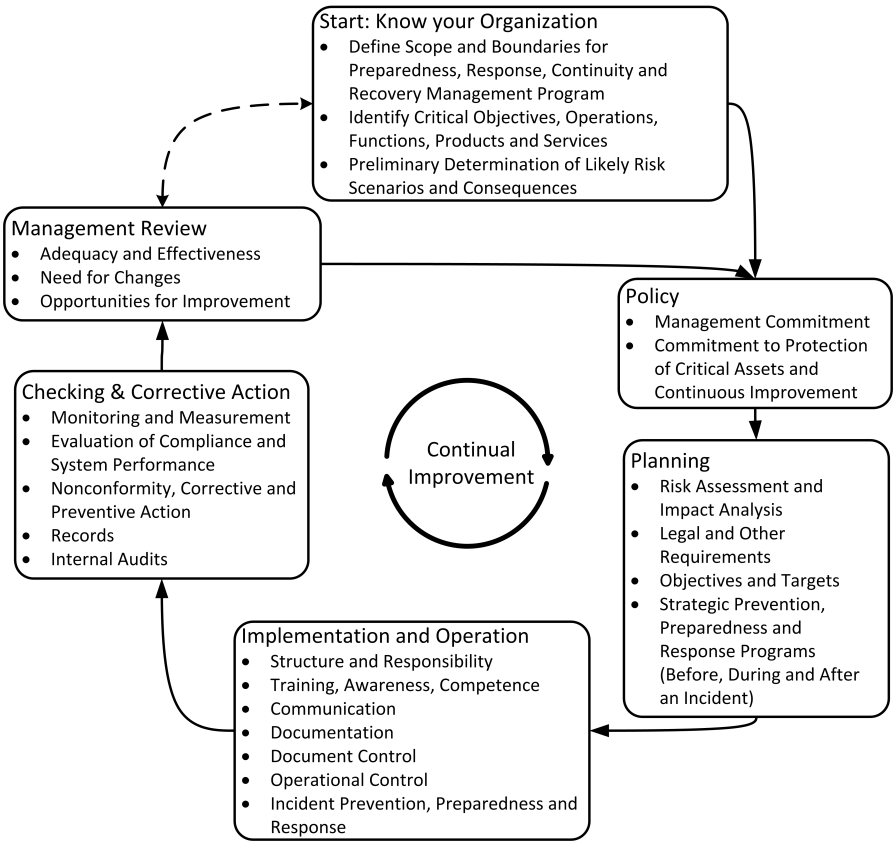

Figure 4.3: ASIS Organizational Resilience Management System Flow Diagram

In Accordance with Blass [2010, p. 4].

phase plays an important role, not only for evaluation of compliance and performance, but also for the improvement of the whole system over time.

The implementation and operation includes clear *resources, roles, responsibility, authority (4.4.1)* and *competence, training, and awareness (4.4.2)* to ensure persons performing resilience management tasks are competent to perform as expected. *Communication and warning (4.4.3)* is a central part at all system levels, as well as *documentation (4.4.4)*, *control of documents (4.4.5)*, *operational control (4.4.6)* and the heart of the standard *incident prevention, preparedness, and response (4.4.7)*.

Summarizing, the overall goal of ASIS is to increase the organizational resilience through systematic planning, action, control and improvement of a predefined resilience framework that can be adopted by any organization.

> *Organizational resilience* [is the] adaptive capacity of an organization in a complex and changing environment; the ability of an organization to resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event; the capability of a system

> to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must.
> [Blass, 2010, p. 48]

The implementation of the prescribed activities, details of information-entities and concrete metrics depend on the line of business, goals of stakeholders and the normative management of an organization. It is a generic standard, that can be extended by other standards and includes softer cultural aspects as well as hard aspects like *control in the small*.

4.2.2 The CERT Resilience Management Model

The CERT Resilience Management Model (CERT-RMM) is the first know model that includes a capability dimension on resilience management processes, enabling planning and control of operational resilience management processes[6] through resilience metrics. This allows to predict how an organization will perform under stress, disruption and changing environments [Caralli et al., 2010a, p 2]. The model was developed by Caralli and the Financial Services Technology Consortium from 2004 to 2008. The development team involved companies that have intense knowledge on risk management and business continuity, like JPMorgan Chase and Co, MasterCard Worldwide, The U.S. Bank and others more.

The motivation for the development of the CERT-RMM was the increasing stress on organizations, originating from technology advances that introduce a high level of complexity, the dependence on partnerships, cross-organizational, and geographically distributed supply chains that can be traced back to the high level of economic globalization.

Caralli et al. define operational resilience management as "[...] the ability of the organization to achieve its mission even under degraded circumstances [...]", [2010a, p. 1]. A further definition they use is: "[...] the emergent property of an organization that can continue to carry out its mission after disruption that does not exceed its operational limit.", [2010a, p. 1]. Further relevant semantic definitions of core concepts are quoted subsequently.

> [*Operational Resilience* is] the organization's ability to adapt to risk that affects its core operational capacities. Operational resilience is an emergent property of effective operational risk management, supported and enabled by activities such as security and business continuity. A subset of enterprise resilience, operational resilience focuses on the organization's ability to manage operational risk, whereas enterprise resilience encompasses additional areas of risk such as business risk and credit risk.
> [Caralli et al., 2010a, p. 848]

> *Operational resilience management* defines the processes and related practices by which an organization designs, develops, implements, and controls strategies for protecting and sustaining critical high-value services, related business processes,

[6] The *CERT-RMM* bases on the industry and scientific experience on process quality management. The model uses the fact that the quality of a system or service is strongly influenced by the quality of the underlying processes [Caralli et al., 2010a, p. 3].

Engineering		**Operations**	
AD	Asset Definition and Management	AM	Access Management
CTRL	Controls Management	EC	Environmental Control
RRD	Resilience Requirements Development	EXD	External Dependencies Management
RRM	Resilience Requirements Management	ID	Identity Management
RTSE	Resilient Technical Solution Engineering	IMC	Incident Management and Control
SC	Service Continuity	KIM	Knowledge and Information Management
		PM	People Management
		TM	Technology Management
		VAR	Vulnerability Analysis and Resolution
Enterprise Management		**Process Management**	
COMM	Communications	MA	Measurement and Analysis
COMP	Compliance	MON	Monitoring
EF	Enterprise Focus	OPD	Organizational Process Definition
FRM	Financial Resource Management	OPF	Organizational Process Focus
HRM	Human Resource Management		
OTA	Organizational Training and Awareness		
RISK	Risk Management		

Table 4.1: Process Areas of the CERT Resilience Management Model

> and associated assets.
> [Caralli et al., 2010c, p. 1166]

> [*Operational risk is*] the potential impact on assets and their related services that could result from inadequate or failed internal processes, failures of systems or technology, the deliberate or inadvertent actions of people or external events.
> [Caralli et al., 2010c, p. 1166]

Processes, Assets, Services and Capability Metics

Caralli et al. [2010a, p. 20] adduce three core elements of the operational resilience management model: *assets, processes*, and *services*. Assets can be people, information, technology and facilities. These assets are used and combined within business processes. Business processes, again, act in concert to provide one operational service. They define a service as "the limited number of activities that the organization carries out in the performance of a duty or in the production of a product", [2010a, p. 21].

The CERT-RMM consists of *26 process areas*, visualized on Table 4.1, out of the four resilience management areas: *engineering*, *operations*, *process management* and *enterprise management* [Caralli et al., 2010a, p. 3].

From Resilience Goals to Requirements, Practices and Metrics

Caralli et al. declare that resilience requirements derive from resilience goals and objectives. Those goals and objectives derive from organizational drivers and the corresponding risks on them. Resilience requirements include the definition of protection strategies and controls as well as sustainment strategies and controls. These strategies and controls are applied to the high-value assets derived from high value services and organizational drivers. "Resilience requirements embody the strategic objectives, risk appetite, critical succes factors, and operational constraints of the organization", [Caralli et al., 2010a, p. 26]. *Protect strategies* minimize the probability that an asset will be exposed to sources of disruption [Caralli et al., 2010a, p. 26]. *Sustain strategies* have the target to keep assets operating during stressful or disruptive incidents possibly close to operations under normal conditions [Caralli et al., 2010a, p. 27]. Each of the 26 process areas, listed in Table 4.1 includes *specific goals* for resilience. A specific goal includes specific practices that support the achievement of the goal. The CERT-RMM includes specific metrics to measure the fulfillment of specific goals and specific practices [Allen and Curtis, 2011; Allen and Davis, 2010].

The specific practices of a process area contain an even deeper recursion of practices: the specific subpractice. Each specific practice contains several specific subpractices. According to Partridge et al., these subpractices constitute exemplary work-products that serve to fulfill a specific practice. The *specific subpractices* are optional elements and *constitute the interface to other management standards* that are related to resilience management: for example the ISO 31000:2009 Risk Management Standard. The ASIS SPC.1-2009 Resilience Management Model, the ISO 27002:2005 Information Security Standard and the BS25999-1:2006 Business Continuity Standard [Partridge and Young, 2011]. Each of these standards can be used in combination with the CERT-RMM. The defined activities of the related management standard are used as specific subpractice in the CERT-RMM.

All in all, the CERT-RMM is a very broad approach of operational resilience management focusing on process capability as preparation for crises, hazards and any type of severe incident. The model is open for the integration of related best practice models and standards. This raises the chance, that the concept of resilience metrics and resilience process capability might also be an useful element for the cybernetic frameworks that will be developed in Chapter 5.

4.3 Key Findings

KEY FINDINGS

- Organizational resilience requires a combination of foresighted planning before and flexible improvisation during a crisis.
- When organizational structures like role systems get destroyed, a sensemaking process must be initiated to rebuild meaning and a new structure in succesion.
- When meaning is lost in an organization, structure is necessary for rebuilding the meaning.
- The ASIS SPC.1-2009 Organizational Resilience Management Standard is the most generic and comprehensive model for resilience management.
- The CERT Resilience Management Model provides metrics for assessing the capability of resilience activities from different fields of enterprise management.

ANSWER TO RESEARCH QUESTION 2

1.1 How does the scientific and industrial management community define organizational resilience?

- *Organizational resilience is the maintenance of positive adjustment under challenging conditions so that the organization emerges strengthened and more resourceful from adverse conditions (adopted from Sutcliffe and Vogus [2007]).*

1.2 How does the scientific and industrial management community define organizational resilience management?

- *Organizational resilience management includes systematic and coordinated activities and practices through which an organization manages its ability to adapt to risks, the associated potential threats and impacts (adopted from Blass [2010]; Caralli et al. [2010a]).*

CHAPTER 5

Development of an Enterprise Risk and Resilience Management Framework

" Policy-making, decision-making and control: These are the three functions of management that have intellectual content. "

[Anthony Stafford Beer, 1926 - 2002.]

Contents

5.1 Cybernetic Risk Management Framework **46**

5.2 Cybernetic Resilience Management Framework **57**

5.3 Comparison of Risk and Resilience Management **69**

5.4 Integrated Enterprise Risk and Resilience Management Framework **72**

Abstract This chapter is divided into four distinct sections.[1] The first section includes the development of a cybernetic risk management model. The second section is an elaboration of a cybernetic resilience management model. The third section compares the two developed models to find common parts and distinctions. In the fourth section risk an resilience management are integrated into one enterprise-wide cybernetic management framework.

[1] **Citation style for Chapter 5**: The citation style for this chapter differs from the normal style in the thesis, as references by page number would be too imprecise for the applied semantic content analysis. In order to refer to exact terms out of a certain reference the cited terms are emphasized and labeled with the corresponding number from the original document; for example: *risk attitude (2.5)*. Which literature a citation refers to, is explained in the beginning of the following sections.

5.1 Cybernetic Risk Management Framework

In this section the semantic content of the ISO 31000 Risk Management Standard is analyzed in detail. This analysis allows to identify the core elements of the standard - information, action, flow of information as well as planning and control cycles - and to model them as Cybernetic Management Framework (CMF). The analysis of the planning and control cycles bases additionally to the semantic analysis on the risk management process visualized in Figure 3.3.[2]

There are several reasons why the choice of a risk management standard as model for this section fell on ISO 31000: In the first place Schwaiger already modeled the COSO ERM Framework in his work [2012]. In the second place the ISO 31000 Standard has the goal to increase resilience (see Table 3.1). So, this standard is a good choice as foundation for the later development of an integrated risk and resilience framework. In the third place the Global ISO 31000 Survey [G31000, 2012] revealed that ISO 31000 is more diffused than COSO among practitioners and enterprises, what is another good reason to model it.

5.1.1 Analysis of Activities, Information Flow and Levels of Control

This section provides an overview over the processes, management cycles and main information flow between the activities within management and business systems. The cybernetic view on ISO 31000 is illustrated in Figure 5.1 as Cybernetic Management Framework. The visualization is and extension of Management Activity Diagrams through the inclusion of different hierarchical levels of enterprises. The subsequent paragraphs include the description of core risk management activities[3] on these hierarchical levels.

(1) Plan-Activity: The plan-activity does establish the *context* (2.9), namely the *internal context (2.11)* and the *external context (2.10)*. The external context is related to key drivers and trends that have impact on the organization and relationships with *external stakeholders (2.13)*. The internal context includes the *risk profile (2.20)* for the organization or parts of the organization and the related *risk criteria (2.22)* based on external and internal context. Concerning the internal context, the *risk management policy (2.2)* and the *risk attitude (2.5)*, that are usually provided beforehand by the normative management, can - under certain conditions - be re-planned in accordance with normative and strategic management levels.

(2) Measure-Activity: The *risk identification (2.15)* and *risk analysis (2.21)* are successional parts of this activity.

Risk identification serves to find, recognize and describe *risks (2.1)* as well as the according *risk sources (2.16), events (2.17)* and *potential consequences (2.18)* of realized risks. If the PDCA-Cycle has already run through at least once, it is possible that risks had already been treated, but some of them remained. A risk that remains after risk treatment is called *residual*

[2] **Citation source for Section 5.1:** In this section emphasized references including numbers beween brackets refer to elements the ISO 31000 Risk Management Standard [2009].

[3] I have elaborated parts of the sections 5.1.1 and 5.1.2 as first draft in the lecture "IT Based Management" at the Vienna University of Technology in 2011.

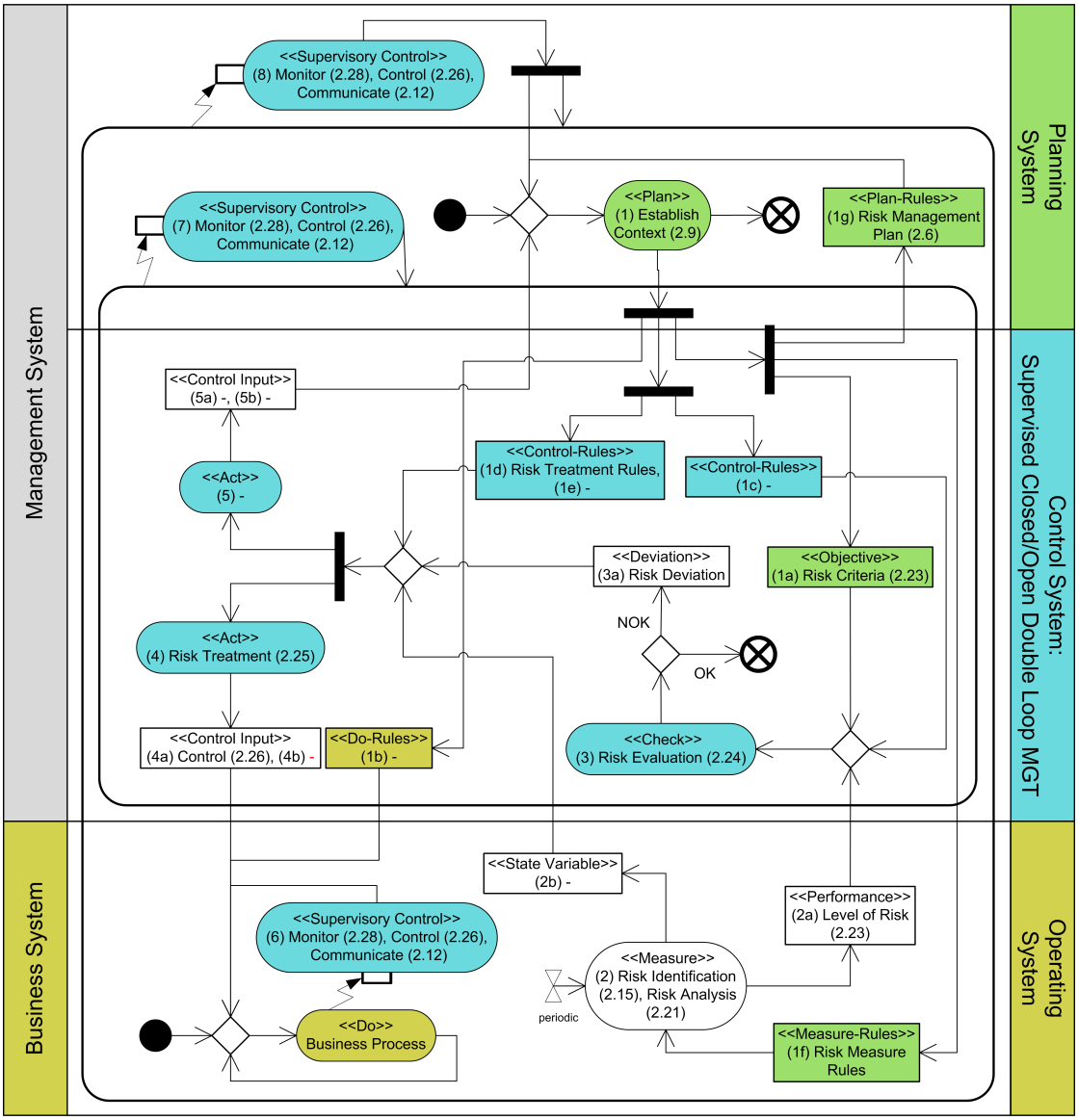

Figure 5.1: The ISO 31000 Risk Management Process Modeled as Cybernetic Management Framework

risk (2.27) and can also be identified in this activity. The risk analysis serves to comprehend the *nature of risks (2.1)* or *residual risks.*[4] *(2.27)* and to determine the *level of risks (2.23)*.

[4]The term *residual risk* will not be used explicitly in later elaborations, as the risk management activities in the ISO 31000 standard do not depend on whether the risk is new or a residual one.

(3) Check-Activity: The *risk evaluation process (2.24)* serves to determine whether the *risk (2.1)* and its *risk level (2.23)* are acceptable or tolerable by comparing the results of the *risk analysis (2.21)* with the predefined *risk criteria (2.22)*.

(4) Corrective Act-Activity: The *risk treatment (2.25)* modifies *risk (2.1)* by removing the *risk source (2.16)*, changing the *likelihood (2.19)* or the *consequences (2.18)* of the risk.

(5) Adaptive Act-Activity: The core principles of the ISO 31000 standard comprise *dynamic responsiveness to change, organizational learning* and *continual improvement of the organization*, but there exists no explicit definition of an adaptive act-activity in the sense of second order learning.

(6) Process Supervision-Activity: *Monitoring (2.28)* checks, supervises, observes and determines the status of a *risk (2.1)* and a *risk control (2.26)* in order to identify change from the expected performance level. *Review (2.29)* determines the suitability, adequacy and effectiveness of the *risk (2.1)* and *risk control (2.26)*. *Communication and consultation (2.12)* provides, shares or obtains information and engages the dialogue with *stakeholders (2.13)* regarding the management of *risks (2.1)*.

(7) Control Supervision-Activity: *Monitoring (2.28)* checks, supervises, observes and determines the status of the *risk management process (2.8)* in order to identify a deviation from the expected performance level. *Review (2.29)* determines the suitability, adequacy and effectiveness of the *risk management process (2.8)*. The *communication and consultation (2.12)* activities provides, share or obtain information and engage the dialogue with *stakeholders (2.13)* regarding the management of risks (2.1).

(8) System Supervision-Activity: *Monitoring (2.28)* checks, supervises, observes and determines the status of the *risk management framework (2.3)* in order to identify deviations from the performance level required or expected. *Review (2.29)* determines the suitability, adequacy and effectiveness of the *risk management framework (2.3)*. Again, *communication and consultation (2.12)* provide, share or obtain information and engage the dialogue with *stakeholders (2.13)* regarding the management of *risks (2.1)*.

5.1.2 A Risk Management Ontology

This section contains the elicitation of all core entities of the ISO 31000 standard. Data objects are described and depicted below as elements of class diagrams. Data objects that are not explicitly defined in the ISO 31000 standard, but clearly, syntactically derive from the written standard, are also depicted in this section. In order to distinguish between those explicit and implicit data objects of the framework, the implicit ones do not have a reference number between brackets. The risk management ontology of the ISO 31000 Standard is visualized in Figure 5.2.

Objects Related with the (1) Plan-Activity

(1a) Objectives: Objectives are defined in the *risk criteria (2.22)* containing information like risk tolerance for different risk types and objectives of the internal, respectively external context.

(1b) DO-Rules: DO-rules concern the special business processes that are observed. As no special business processes are part of the ISO 31000 standard, the DO-rules are not defined in this standard.

(1c) CHECK-Rules: The ISO 31000 Risk Management Standard can be applied to the management of any risk within any enterprise, independent of its line of business. The CHECK-rules are not explicitly defined in the standard as they have to be designed and implemented by the actual firm depending on its internal and external business context.

(1d) Corrective ACT-Rules: The risk treatment rules are not explicitly defined in the standard, but result out of the (1) planning process.

(1e) Adaptive ACT-Rules: see (2b)

(1f) Measure-Rules: Risk measure rules are not explicitly defined, however clearly derive from the *risk management policy (2.4), attitude (2.5) and plan (2.6)* throughout the (1) planning process.

(1g) PLAN-Rules: The *risk management plan (2.6)* includes the risk management scheme, approach, resources and components (procedures, practices, assignment of responsibilities, sequence and timing of activities).

(2a) Performance Measure: The *level of risk (2.23)* specifies the magnitude of *risk (2.1)* or a combination of risks. Risks are expressed as a combination of *risk consequences (2.18)* and the corresponding *likelihood (2.19)*.

(2b) State Variable Measure: ISO 31000 underlines the importance of the observation and communicative integration of the *external context (2.10)* including key drivers and trends, however, it does not define how to implement this. As a consequence the elements (2b), (4b), (5b) and (1e) in the Cybernetic Management Framework are left blank. As example for the state variable measure or business environmental information Schwaiger adduces the attractiveness of marks or the competitive advantage [2012, p. 454].

(3a) Deviation: Risk-deviation is due to the comparison of the defined *risk criteria (2.22)* to current *level of risk (2.23)* by using the related context sensitive control rules (1c).

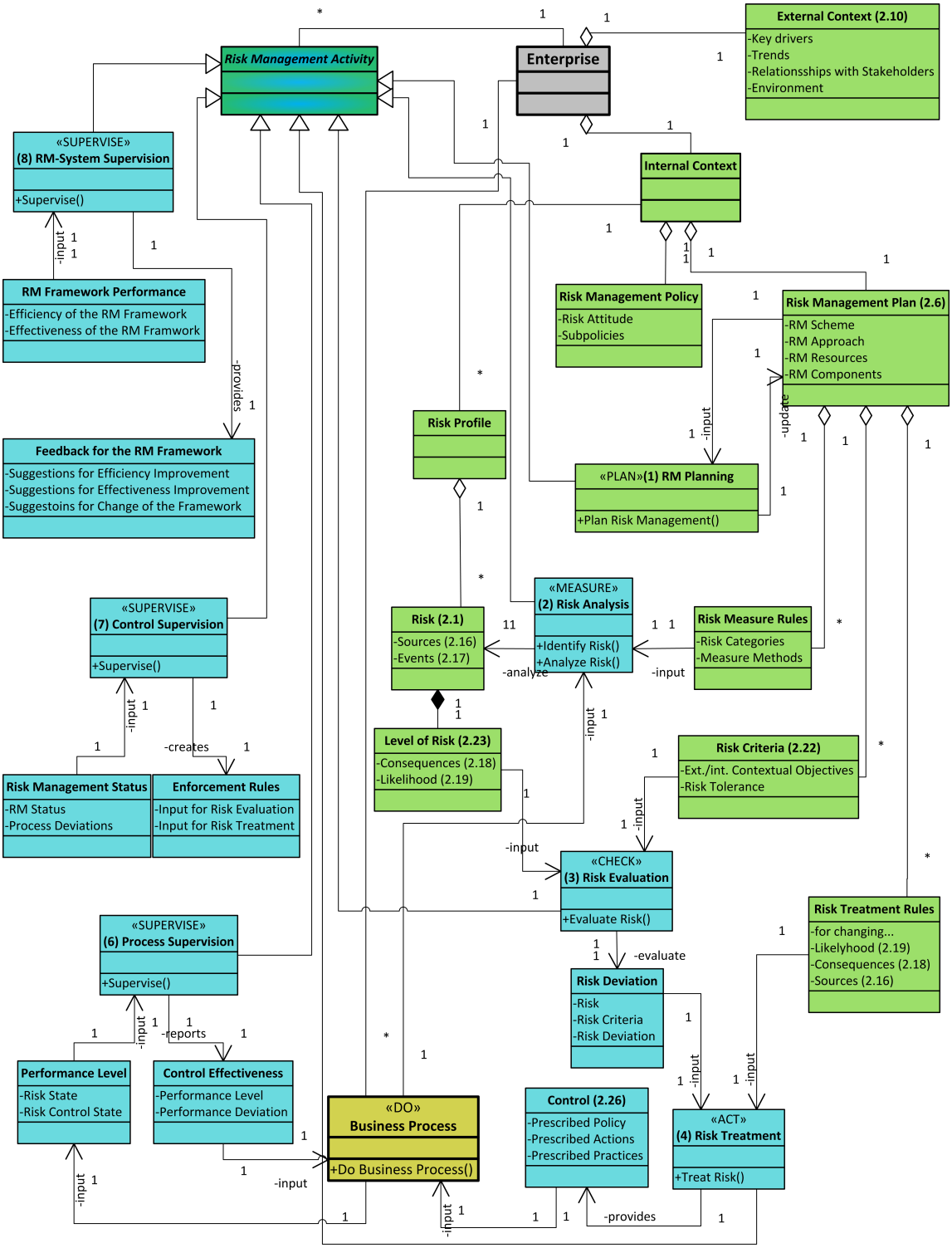

Figure 5.2: The ISO 31000 Risk Management Ontology

(4a) Closed Loop Corrective Control Input: *Control (2.26)* is the prescribed practice, action or measure that will modify *risk (2.1)* and *level of risk (2.23)*.

(4b) Open Loop Corrective Control Input The open loop control input is not explicitly defined in the standard (see 2b). However, it can be derived as the corrective control input for business process management in accordance with changing demands in the business environment modeled and measured as (2b) state variable.

(5a) Closed Loop Adaptive Control Input: The closed loop adaptive control input is not explicitly defined in the standard but can be derived in a semantical-logic way: it is the information entity that evolves from observing, measuring and analyzing the firm-internal risk related business performance and can be used to adapt the ERM system or process in doubt of validity or performance (compare Schwaiger [2012, p. 443]).

(5b) Open Loop Adaptive Control Input: The open loop adaptive control input is not defined in the standard. Again, it can be derived as: information entity that evolves from measuring, analyzing the external context of the firm. The concrete content depends on the design and implementation of the standard (see (5) adaptive act-activity).

(6 Input) Process Supervision Input: This data element is not defined explicitly in the standard, but it can be found in the definition of *review (2.29)*. It is called *performance level* on the basis of current status of *risk (2.1)* and *risk control (2.26)*.

(6 Output) Process Supervision Output: Again, this data element is not defined explicitly, but can be found in the definition of *review (2.29)* under the term of*control effectiveness*.

(7 Input) Control Supervision Input: The *risk management status* is the concerned input. This input is not defined in the ISO standard, but derives from the *monitoring (2.28) definition and allows to monitor the performance status of the risk management processes on the level of the control system.*

(7 Output) Control Supervision Output: *Enforcement measures* provide the knowledge base for the right reactions to process deviations on the control system level. This output is not defined in the standard, but derives from *monitoring (2.28)* as well as the *communication and consultation (5.2)* definition.

(8 Input) System Supervision Input: *Risk management framework performance* can be derived from *monitoring and review (5.6)*.

(8 Output) System Supervision Output: *Feedback for the risk management framework* can also be derived from *monitoring and review (5.6)* as well as *communication and consultation (5.2)*.

5.1.3 Evaluation of the Framework

The ISO 31000 Risk Management Standard focuses on the *prevention of risk realizations* and the *preparedness for risk realizations*. The prevention can be done by reducing the likelihood of a potential risk event or by reducing the impact of potential risk events. The preparedness shall ensure that the organization and the business units increase the probability of successfully surviving realized risks. The encompassing risk management of ISO 31000 includes different management cycles, as defined in the Cybernetic Management Framework. The implementation of these management cycles is evaluated below.

Open and Closed Loop Risk Management

The focus of ISO 31000 is on the *closed loop control cycle* by combining the likelihood and consequences of potential risk events to the *level of risk (2.23)* on business processes. Schwaiger explains that the corrective act-activity in ERM has the purpose of *business performance management* over economic sub-periods of an organization [2012, pp. 444-445]. An explanation: as risk management supports the achievement of business goals in a direct way, risk management can be treated as synonym for performance management. In the closed loop control cycle of the CMF business management and risk management (alias performance management) are combined. As conclusion the closed loop control cycle is named business performance management.

The *open loop control* cycle is theoretically part of the standard, by observing and reacting to changes in the *external context (2.10)*, however, no details are provided on how to implement this. Possible examples for external indicators could be the market attractiveness, the size or growth of the market and the structure of the competitive environment. These indicators can be measured as (2b) state variable.

First and Second Order Learning

First order learning allows to adapt business processes by analyzing the business system and providing new control input. This includes a control system observing and modeling the business system as (2a) performance measure and the business environment as (2b) state variable over the run of time. On the basis of these observation, new control input is provided for the business system. The core process, besides (2) risk measuring and (3) risk evaluation, happens in the *(4) corrective act-activity*.

Second order learning enables the organization to review the whole risk management system and associated processes. The main action of second order learning happens in the *(5) adaptive act-activity* which can be defined in the style of Schwaiger's reasoning: if risk deviations cause doubt of validity the second order learning process is initiated by the adaptive act-activity for re-calibration or re-construction of the risk models, what involves a *"permanent cybernetic model for life cycle management"*, [2012, p. 443]. However, the actual activities and the related information flow (5a, 5b) has to be defined by the organization that designs and implements the ERM system.

Pro- and Reactive Risk Management

Reactive risk management is a central part of the ISO 31000 standard through changing the business system by (4) corrective actions or by changing the risk management system by (5) adaptive actions. These actions are reactions to deviations of already realized risk levels to planned risk levels or of already realized external changes like the competitive environment.

Schwaiger defines *proactive risk management* as the achievement of business objectives by *stochastic forecasting* of future performance of business processes on the basis of the performance indicators of realized sub-periods. He explains further, that especially in the adaptive-act activity proactivity plays a central role, by anticipating changes of external market indicators and using them as open-loop feedforward information (5b) to adapt the whole ERM system to sustain competitive advantage. Although, *risk identification (5.4.2)* includes risks with sources that are not under the control of the organization [ISO, 2009, p. 18] and identification or risks includes what might happen this does not satisfy the definition of Schwaiger's proactive approach. Nevertheless, the stochastic control theory can be included in the developed framework, as Schwaiger does for the COSO Enterprise Risks Management Framework [2012].

The evaluation reveals that reactivity is more an issue of compliance, process quality and functional validity, what adds indirect value to business performance, whereas proactive risk management adds direct value to the business performance and can easily be added by using stochastic control theory.

Comparison to the COSO ERM Framework

In the subsequent paragraphs the core elements of COSO are compared to ISO 31000 to find out whether COSO could add additional valuable elements or attributes to the elaborated framework.

The COSO Enterprise Risk Management Integrated Framework consists of eight interrelated components [2004, pp. 3-4].

1. The *internal environment* including the risk management philosophy, appetite and ethical values can be compared to the *internal context (2.11)*.

2. The *objective setting* means that objectives must exist before risk events can be identified. The objective settings must be aligned with the entity's mission and risk management philosophy. The objective settings can be mapped to the *risk management plan (2.6)* including the *risk criteria (2.22)*, both being a subpart of the *internal context (2.11)*.

3. *Risk identification* of internal and external events that have impact on the entity's objectives including risks and opportunities can be compared to *risk identification (2.15)*.

4. *Risk assessment* analyzes risks including likelihood and impact. It can be compared to the following successional activities: *risk identification (2.15), risk analysis (2.21)* and *risk evaluation (2.2.4).*

5. *Risk response* includes avoiding, accepting, reducing or sharing risk, again, aligned with the entity's risk appetite. It can be compared to *risk treatment (2.25)*.

6. *Control activities* ensure that risk responses are carried out effectively. They can be compared to the *control (2.26)* activity.

7. *Information and communication* ensures the duly identification, capturing and sharing of information. It can be compared to *communication (2.12)*.

8. *Monitoring* and evaluation of the whole enterprise risk management system permits necessary modifications of the whole system. It can be compared to the *monitor activity (2.28)*.

All components if COSO can be identified in ISO 31000. So, COSO can not add additional, constitutional, valuable elements to the designed framework.

COSO includes four distinct categories of risk management objectives: strategic, operations, reporting and compliance objectives [2004, p. 3]. Although, the categories are distinct, they are strongly interlinked and goals can be part of more than one category.

1. *Strategic objectives* include top level goals derived from the organization's mission. They can be compared to the *risk management policy (2.2)* including the *risk attitude (2.5)*, as the *risk management framework (2.3)* is embedded within the strategic policies of the organization.

2. *Operations objectives* aim to the efficient and effective employment of different types of resources. They relate to the achievement of an entity's core mission including choices related to structure and performance of the entity. The core focus of ISO 31000 is on strategic and operational risk objectives, Although, operational risk objectives are strongly interrelated with operational business objectives, the concept of ressource allocation is not a main element of ISO 31000.

3. *Reporting objectives* ensure the reliability of the enterprise risk management reporting system. In ISO 31000 the reporting processes and objectives are build up in *establishing internal (5.3.1) and external (5.3.2) communication and reporting mechanisms (4.3.6)*. Within *monitoring and review (5.6)* the achievement of reporting objectives is measured.

4. *Compliance objectives* ascertain the compliance with different laws and regulations that apply for the enterprise. *Risk criteria (2.25)* are derived from laws, policies and other requirements [ISO, 2009, p. 5]. In the introduction phase of the ISO risk management system the management ensures the legal and regulatory compliance within the following activities: *mandate and commitment (4.2)*, *understanding of the organization and its context (4.3.1)*, and *establishing the internal (5.3.3) and external context (5.3.2)*. Through the lifecycle of the risk management system in *monitoring and review (5.6)* necessary adaptions are implemented by *re-establishing the context (5.3)*, as illustrated in Figure 3.3.

The inclusion of compliance, reporting and strategic objectives is fully satisfied by the ISO 31000 standard. Although the ISO framework shall be seamlessly included in the enterprise management on strategic and operative level, the operations objectives are not an explicit part of the framework.

Risk Types and Risk Management Culture

Kaplan and Mikes conducted intense casestudy research on enterprise risk management in financial institutions and came up with a new typology of risks [2012; 2013]. They argue that their categorization is a necessary foundation for the solution of currently dominating problems in ERM. The developed cybernetic risk management framework, and thereby ISO 31000, is now evaluated against the management of these risk categories.

1. *Preventable risks* that have its source within the organization are controllable to a high extend and can be managed perfectly using the developed cybernetic framework including Schwaiger's stochastic control theory for proactive risk management [Schwaiger, 2012]. These risks are related to inappropriate action of employees, the breakdown of operational processes and are best managed by monitoring and enforcement [Kaplan and Mikes, 2012, p. 52]. In ISO 31000 *risk treatment (2.25)* involves avoiding, removing the risk source, changing likelihood, changing consequences, sharing, retaining riks.

2. *Strategy risks* are accepted by a company to generate superior returns [Kaplan and Mikes, 2012, p. 53]. According to Kaplan and Mikes these risks are, in contrast to preventable risks, not undesirable, however, they can not be managed through sole rule-based planning and control. In ISO 31000 risk treatment (2.25) includes *taking or increasing risk* to pursue a strategy that creates increased profit through competitive advantage. The assessment of strategy risks requires, as part of the planning and control framework, special methods to envision risks which are not included in the ISO standard. These methods are interactive discussions between experts, maps of likelihood and key risk indicator scorecards [Kaplan and Mikes, 2012, p. 47].

3. *External risks* arise outside of the company and are beyond its influence. The risk management of this risk category shall focus on the identification and mitigation of their impacts [Kaplan and Mikes, 2012, p. 53]. Power claims that ERM systems are unable to process external systemic risks, "since this would require an imagination of externalities well beyond their design parameters", [2009, p. 853]. The view on the semantic level of the ISO 31000 concept shows the envisioning of risks [Kaplan and Mikes, 2012, 2013] is indeed part of the standard. However empirical surveys have shown, that the implementation of ISO 31000 in real life companies often lack this sub-approach [Mikes, 2011, 2009; Power, 2009].

In its ideal conception ISO 31000 is *a holistic risk management system* in the sense of Mikes' categories of risk management systems presented in Section 3.2.2. ISO 31000 includes the goals of measuring both, internal and external risks, in a quantitative and qualitative way. It includes principles like perpetual reflection and renewal in the sense of an adaptive learning organization. These elements make up the holistic approach driven by risk based internal control, which were promoted by the european and american legislation within the last decade. However, the holistic approach is a theoretic conception and it becomes clear that the management of the three distinct risk types is, in real business life, related to the *dominating risk management culture* of a firm, like risk enthusiasm and risk pragmatism [Mikes, 2011, 2009]. Therefore, a further evaluation of

the application of ISO 31000 in real organizations would be necessary to approve the conception. Several researches conducted these empirical surveys and came to the results presented in the following paragraphs.

Power blames the current ERM systems to focus on quantitative methodologies where the risk appetite is a singular input into the system, reflecting a thermostatic conception [2009, p. 851].

> At the heart of the machine idea the category of 'risk appetite' names the value inputs which, in theory, prescribe triggers, limits and tolerances for feedback and control purposes. For example standards like those of COSO define risk appetite as the amount of risk and entity is willing to bear. [...] Although, COSO [annotation: and ISO 31000 as well, as they base on the same principles] envisages the possibility of 'qualitative' understandings of risk appetite, the dominant conception is that of a quantitative benchmarks [...].
> [Power, 2009, p. 850]

In his opinion risk appetizing is nothing more than an organizational process, with risk appetite as exogenous input, missing a more meaningful ecology of values [2009, pp. 851, 854]. He finds that risk appetite was gets lost within organizational details of the planning and control paradigm, as "no individual person, or group of persons, calling themselves accountant, is responsible and blameworthy [...]", [2009, p. 854].

KEY FINDINGS

- The developed framework satisfies most elements of COSO ERM, except the attributes of organizational entity-levels and the operational objective type. The concept of operational objectives and resources management will be part of Section 5.2 on resilience management. The attribute of entity-levels will be integrated in the later Section 5.4 on cybernetic enterprise management.
- The framework has the conceptual potential to be a holistic risk management framework, but in real business life quantitative enthusiasm with a focus on high trust in mathematical modeling is dominating.
- For the reasonable management of strategic risks a mix of qualitative and quantitative risk management culture is necessary.
- For the sensible management of external risks tools for envisioning in a qualitative and quantitative way should be integrated.

ANSWER TO RESEARCH QUESTION 2

1.1 Which activities, information and information flow shall a cybernetic management framework for risk management include?

- *See Figures 5.1 [p. 47], 5.2 [p. 50] and the related description.*

5.2 Cybernetic Resilience Management Framework

Organizational resilience management is a rather young industrial and scientific domain and only few resilience management models exist. The two most elaborated concepts are the ASIS SPC.1-2009 Organizational Resilience Management Standard [Blass, 2010] and the CERT Resilience Management Model (CERT-RMM) [Caralli et al., 2010b]. Whereas the CERT-RMM focuses on a very comprehensive collection or resilience management processes and related resilience metrics, the ASIS standard incorporates a more generic and cybernetic approach. ASIS focuses on the planning and control cycles as well as the embedding of resilience management in the organizational management context, whereas CERT-RMM relies on a huge collection of operational resilience management processes that can be used for measuring the process capabilities of resilience management processes.

The cybernetic approach of ASIS appears to be best suitable for being modeled as Cybernetic Management Framework, as it focuses intensively on first and second order control cycles and supervisory control, what are the core elements of the CMF. The process capability approach will be included in Section 5.4 in terms of metrics on the ASIS and ISO 31000 management processes that are modeled in this and the previous section.

In the subsequent elaborations a semantic analysis[5] of the ASIS standard on organizational resilience is conducted. The core elements of the standard - information, action, flow of information as well as planning and control cycles - are modeled as Cybernetic Management Framework (CMF). The analysis of the planning and control cycles bases additionally on the ASIS resilience management system flow (see Figure 4.3).

5.2.1 Analysis of Activities, Information Flow and Levels of Control

The activities, the information flow and the levels of control are modeled as cybernetic resilience management framework in Figure 5.3. The involved resilience management activities are listed and described in the following paragraphs.

[5] **Citation source for Section 5.2:** Emphasized words with succeeding numbers within brackets refer to the original definitions in the ASIS standard [Blass, 2010]. Emphasized words with preceding numbers between brackets (like *(1) Plan-Activity*) refer to the newly developed Cybernetic Resilience Management Framework that is illustrated on Figures 5.3 and 5.4.

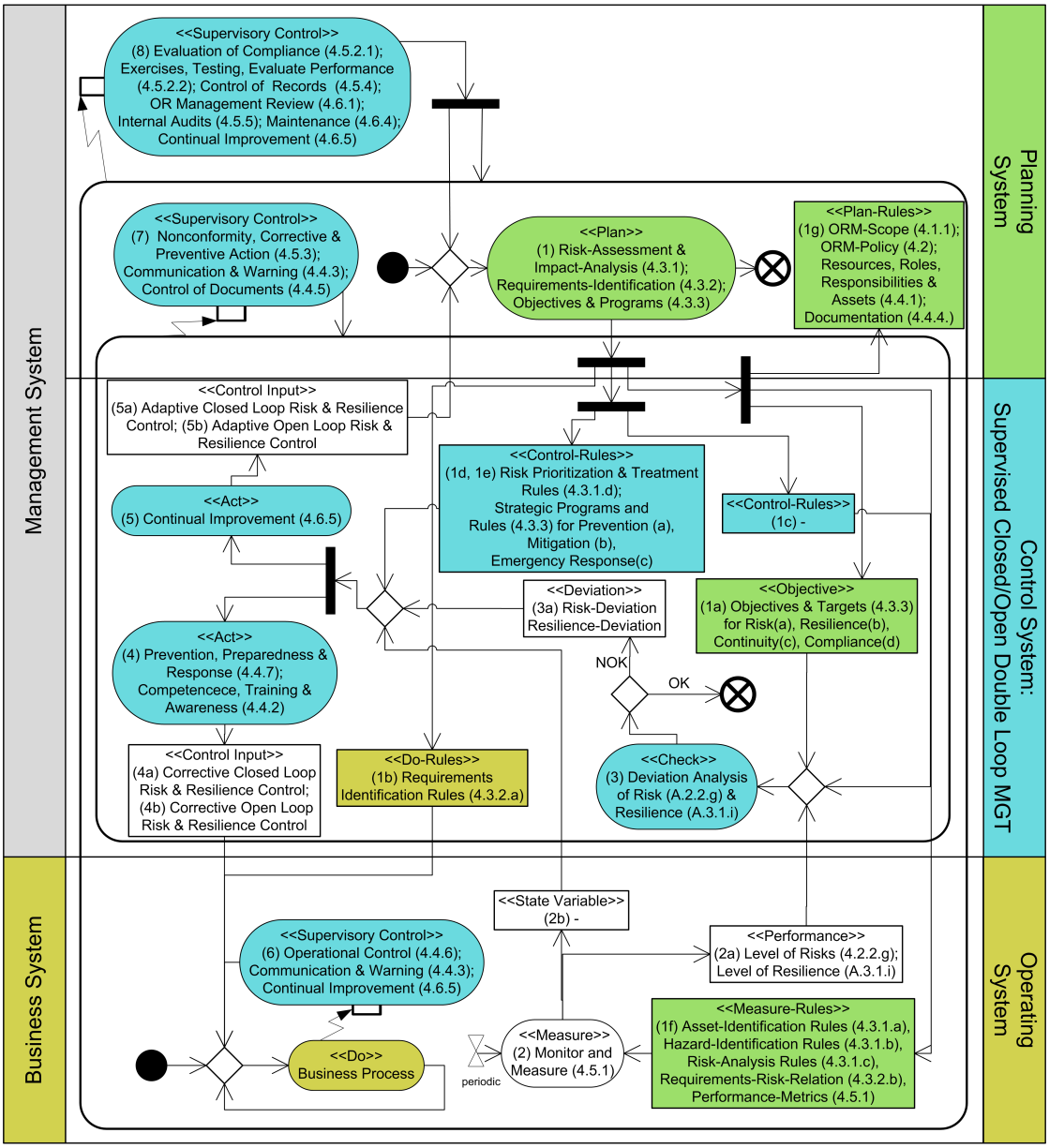

Figure 5.3: The ASIS Resilience Management Standard Modeled as Cybernetic Management Framework

(1) Plan-Activity:

The first subtask within the plan activity is to establish, implement and maintain *risk assessment and impact analysis processes (4.3.1)* that enable the resilience management team to identify core-assets, potential hazards and threats; to analyze risks, vulnerability, criticality, impacts and

related consequences; the prioritization of risk controls and treatments including related costs as well as the determination of risk significance in relation to the potential impact on assets [Blass, 2010, p. 7].

The second subtask within the plan activity is to establish and maintain *procedures for the identification of legal and other requirements (4.3.2)*. These procedures let the resilience management team identify requirements and determine how the different requirements apply to hazards, risks and their potential impacts [Blass, 2010, p. 7].

The third subtask within resilience management planning is to establish and maintain *qualitatively and quantitatively measurable and documented objectives and targets (4.3.3)*. These objectives apply for risk prevention, reduction and mitigation; resilience enhancement; business resilience; compliance with requirements; and continual improvement of the resilience management framework [Blass, 2010, p. 8].

(2) Measure-Activity: *Monitoring and measurement (4.5.1)* analyzes the "characteristics of operations that have material impact on its performance (including partnership and supply chain relationships)", [Blass, 2010, p. 14]. The inclusion of parnerships and supply chains relationships shows that the ASIS standard explicitly includes the measurement and modeling of external conditions as (2b) state variable. The detailed measure activities are not defined, but can be semantically derived by *risk assessment and impact analysis (4.3.1)* as: *asset identification*, *risk identification*, *hazard identification*, *risk analysis*, *risk prioritization*, *identification of requirements-risk-relations*, *performance measurement*. So, ASIS involves, additionally to business performance and risk measurement, a strong focus on critical asset and hazard identification.

(3) Check-Activity: In the ASIS standard no concrete check activities are defined in the sense of the Cybernetic Management Framework. However, after analyzing the *(2) measure-activity*, the performance elements and therewith the check-entities become clear: *level of risks (A.2.2.g) deviation analysis* and *level of resilience (A.3.1.i) deviation analysis*.

(4) Corrective Act-Activity: The main corrective resilience management actions are split up into *(4.1) prevention, (4.2) preparedness and (4.3) response (4.4.7); competence, training and awareness (4.4.2).*

Prevention (4.1) starts with the risk treatment of potential risks that have been identified and measured before. The risk treatment options include *reducing the likelihood of a potential risk event* and *minimizing the impact of a potential risk event*. Detailled *risk treatment options (A.4.7.a.ii)* are "[...] avoidance, elimination, reduction, spreading, transfer, and acceptance strategies", [Blass, 2010, p. 30]. The reduction of likelihood can be done by avoidance or elimination of the risk sources. The reduction of impact can be done by minimizing the effects of a risk event, by spreading the effects over different assets or by transferring the risk to another party [Blass, 2010, p. 30]. Prevention includes proactive steps[6] to coordinate, share information,

[6]The proactive note of prevention and preparedness is due to the involvement of envisioning future risk events. However, it may not be mixed up with Schwaiger's concept of proactive management [2012]. Schwaiger uses the term proactivity in the sense of stochastic control theory where planned objectives are compared to stochastically

protect physical key assets, control access, increase awareness and readiness by training, warning and alarm systems as well as practices to reduce threats [Blass, 2010, p. 31]. According to Blass, further elements are to develop an *organizational culture* that enforces the resilience management system, cost effective *mitigation strategies* for different levels of risks and impacts and *reporting to supervisors*. It becomes obvious that prevention has a strong focus on risk management. The business continuity and crisis management aspects are covered by *(4.2) preparedness* and *(4.3) response*.

(4.2) Preparedness includes *physical security system design and planning* and *cost effective mitigation strategies*. Security planning shall protect (a) human life, (b) assets, (c) prevent an escalation, (d) reduce the length of a disruption, (e) restore the operational continuity, (f) recover the normal operations, (g) protect image and reputation. Even though, risk management has the goal to increase preparedness by minimizing the impact of a risk event, the main activities on the operational resilience management level are performed under the title of preparedness.

The *(4.3) response* to a crisis is planned and conducted by the *crisis management team (A.4.7.n)*. Even though, preparedness includes the preparation of crisis management plans, the core activities for crisis management are defined in (4.3) response.

Competence, training and awareness (4.4.2) conducted by the resilience management team shall ensure that all persons that have the potential to prevent, respond to and mitigate risks and hazards become competent and retain records [Blass, 2010, p. 10].

The closed loop control cycle realized by the (4) corrective act-activity implements *continual improvement (4.6.5)* in a first order learning mechanism for the business system.

(5) Adaptive Act-Activity: The core activity within the second order learning cycle of the cybernetic resilience management system is *continual improvement (4.6.5)*. Continual improvement shall ensure, that the whole resilience management system is improved over the run of time, dependent on internal and external changes. It is also part of the different supervision levels (6, 7 and 8) in form of supervised second order learning. One main focus of continual improvement within the (5) adaptive act-activity is to check, whether the processes and rules provided for the first order control cycle are still appropriate. The initiation of continual improvement might be a consequence of policy changes, hazards, changes in business processes, personnel changes, supply chain changes, technology changes or critical lessons learned [Blass, 2010, p. 39].

(6) Process Supervision-Activity: The supervision of the business processes is implemented as *operational control (4.4.6)* for operational processes that are associated with identified risks. This control ensures that processes fulfill the requirements of the organizational resilience management policy, its objectives and targets [Blass, 2010, p. 30].

Communication and warning (4.4.3) "with regard to hazards, threats, risks and the organizational resilience management system", [Blass, 2010, pp. 10–11] includes several activities: (a) documentation, (b) internal communication between levels and functions, (c,d,f) communication with and alerting of stakeholders, (e) adaption and integration of risk or threat advisory system,

forecasted realizations of performance measures. Whether prevention and preparedness is implemented re- or proactive in Schwaiger's sense, depends on the concrete implementation in an organization, however stochastic control theory is not a distinct part of the ASIS standard.

(g,k) the assurement of communication infrastructure during a crisis especially with (h) emergency responders, the assurement of interoperability of responding people and organizations, (j) the recording of information about incidents and related decisions and actions.

Continual improvement (4.6.5) of the business system in terms of first order learning is also part of the process supervision-activity.

(7) Control Supervision-Activities: The control supervision evaluates and updates processes and cycles within the control system. The main control supervision activities *dealing with nonconformity, corrective and preventive action (4.5.3)* include (a) the identification of nonconformities, (b) of causes, (c) the evaluation of need for action to prevent reoccurrence, (d) the recording of taken preventive and corrective actions and (e) the effectiveness-review of corrective and preventive actions. These activities incorporate the continual improvement approach.

Additionally, *communication and warning (4.4.3)* happens on all organizational levels: the business system, the control system and the planning system. For details see (6) Process Supervision Activity.

Continual improvement (4.6.5) of the control system in terms of first order learning is also part of the control supervision-activity.

(8) System Supervision-Activities: System supervision shall evaluate and update the whole organizational resilience management system. The first activity within the system supervision is the *evaluation of compliance (4.5.2.1)* with legal and regulatory requirements. The organization shall evaluate requirements, compare them to industry best practices and keep records of the periodic evaluation results [Blass, 2010, p. 14].

The second activity is to *exercise, test and evaluate the performance (4.5.2.2)* of the organizational resilience management system [Blass, 2010, p. 14]. The target of this supervision is to validate that the system is (a) consistent with the scope of the system and the objectives of the organization based on (b) realistic scenarios. The performance-evaluation shall (c) minimize the risks to assets, the disruption to operations and bring up (d) a report as input for the system. The whole supervision activity (f) is conducted at planned intervals and reviewed for (e) continual improvement [Blass, 2010, p. 14–15].

The third activity *control of records (4.5.4)* shall evaluate the conformity to the requirements of the organizational resilience management system and the ASIS standards. The control of records includes procedures to protect the integrity of records like access, storage, protection and disposal [Blass, 2010, p. 15].

The fourth activity *control of documents (4.4.5)* is also part of the supervision. All documents required for the organizational resilience management system have to be controlled in order to approve the adequacy. Old documents have to be updated or archived if they are no longer used.

The fifth activity *internal audits (4.5.5)* at planned, non-periodic intervals determines whether the procedures, objectives and controls of the organizational resilience management system comply with (a) the ASIS standard and legislation regulations, (b) the organization's risk management system and (d) perform as expected in (c) an effective way.

The sixth activity is the *general management review (4.6.1)* that evaluates the whole organizational resilience management system to guarantee its suitability and effectiveness. The *maintenance (4.6.4)* of the system ensures that changes in the internal or external context are reviewed and used to adapt parts of the system. The *continual improvement (4.6.5)* of the resilience management system effectiveness is another main part of the system supervision.

5.2.2 Development of a Resilience Management Ontology

This section contains the elicitation of all core entities of the ASIS Resilience Management Standard. Data objects are depicted as elements of class diagrams. Data objects that are not explicitly defined in the ASIS standard, but clearly syntactically derive from the written standard, are also described in this section. In order to distinguish between those explicit and implicit data objects of the framework, the implicit ones do not have a reference number between brackets. The resilience management ontology of the ASIS standard is visualized in Figure 5.4. Due to the complexity of the ASIS standard the ontology is visualized in a compressed way to include all necessary entities. This means that different variants of elements, for example risk, resilience, business continuity and crisis management, are not modeled as distinct objects but as attributes of other objects.[7]

Objects Related with the (1) Plan-Activity:

(1a) Objectives: The objectives consist of distinct *objectives and targets (4.3.3)* for (a) risk prevention, reduction and mitigation; (b) resilience enhancement; (c) financial-, operational- and business-continuity; (d) compliance with legal and other regulatory requirements; and (e) continual improvement. As example for a concrete business continuity objective, ASIS includes the *maximum acceptable outage and recovery time (A.3.1).*

(1b) DO-Rules: *Rules for requirements identification (4.3.2.a).* These are defined processes that allow business units or operative management to identify the core requirements like critical assets. *Asset-identification rules (4.3.1.a)* provide a formal evaluation process to identify the value of the organization's assets like "critical activities, functions, services, products, partnerships, supply chains, stakeholder relationships and their potential impact related to a disruptive incident based on risk scenarios", [Blass, 2010, p. 7]. The identification of these assets can not be conducted by the organizational resilience management team alone, as it requires deep knowledge on concrete business processes, assets and related environments of actual organizational sub-entities.

(1c) CHECK-Rules: Measuring of deviations should be calibrated against traceable national and international measurement standards [Blass, 2010, p. 36]. The concrete rules are not defined in ASIS. Only their necessity and links to possible standards are provided. The analysis of the (2) measure-activity makes clear that there must exist distinct rules for the

[7] Due to the complexity of the ontology the *(5) adaptive action, (1d) adaptive control rules* and *(5a,b) adaptive control input* are not visualized in the ontology, as they add only a minimal extend of information. Details on these elements can be found in the textual description of the ontology.

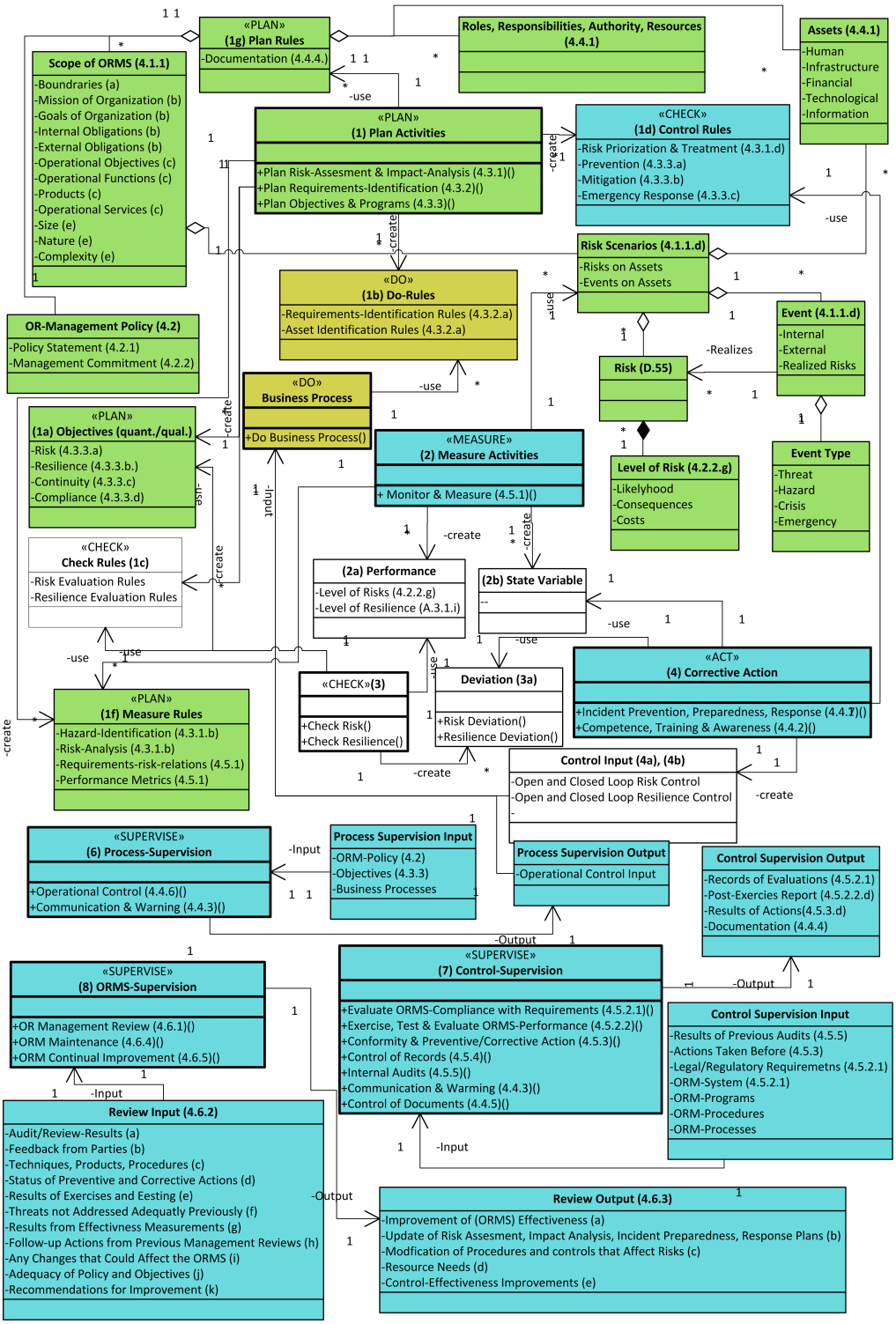

Figure 5.4: ASIS Organizational Resilience Management Ontology

evaluation of risk and resilience deviations. We call them *risk evaluation rules* and *resilience evaluation rules*.

(1d) Corrective ACT-Rules: Include *programs and rules (4.3.3.a) for mitigation; rules and programs (4.3.3.b) to minimize the impact of a disruptive incident; emergency response rules and programs (4.3.3.c);* and *continuity rules and programs (4.3.3.d)*.

(1e) Adaptive ACT-Rules: There exist no concrete control rules for the (5) adaptive-action, as this is a second order learning process that can not be controlled by concrete prescriptions. However, the *organizational resilience management policy (4.2), objectives and targets (4.3.3)* and the *analysis of monitored events and performed corrective and preventive action* serve as normative and historic guidance for the (5) adaptive action (compare *Continual Improvement (4.6.5)* in [Blass, 2010, p. 17]). Due to the complexity of the developed ontology and the limited space the *(1e) adaptive ACT-Rules*, the *(5) adaptive action* and the *(5a, 5b) control input for adaptive action* are not visualized in the resilience management ontology, as they add no concrete important information in comparison to the standard CMF.

(1f) Measure-Rules: *Hazard-identification rules (4.3.1.b)* are formal rules to identify hazards and threats that may have an impact on the operations, functions and assets of the organization. *Risk-analysis rules (4.3.1.c)* enable the systematic analysis of risk, vulnerability, criticality and impacts (consequences) [Blass, 2010, p. 7]. *Requirements-risk-relations (4.3.2.b)* are necessary to find out how different requirements apply to risks, threats, hazards and their potential impact on assets and services. *Performance metrics (4.5.1)* to measure "those characteristics of its operations that have material impact on its performance (including partnership and supply chain relationships)", [Blass, 2010, p. 14].

(1g) PLAN-Rules: The organizational resilience management system *documentation (4.4.4)* is the heart of the plan rules. The documentation includes the following sub-elements: The *scope of the resilience management system (4.1.1)* including (a) boundaries; (b) the mission, goals, internal and external obligations of the organization; (c) operational objectives, assets, functions, products and services; (d) risk scenarios, internal and external events; and (e) the size, nature and complexity of the resilience management system. The *organizational resilience management policy (4.2)* including the policy statement (4.2.1) visualize the commitment to the protection of organizational assets and to the anticipation and preparedness for adverse events as well as business continuity [Blass, 2010, p. 5].

(2a) Performance Measures: The performance measures include the current *level of risks (A.4.3.3.g)*, derived by the term *acceptable level of risks (4.2.2.g)* defined by the top management. The *level of risks (A.4.3.3.g)* is a combination of likelihood of potential risk events and the significance of impacts on assets if they are realized. The second performance measure is the *level of resilience (A.3.1.i)* on critical assets. It defines how resilient an asset stays during the realization of a risk as hazard or crisis. Each realization of a risk as crisis involves *costs of realized risks and crises (A3.1)* that include *human cost (a), financial cost (b), corporate image cost*

(c), economic losses to the community in which the organization operates (d) and environmental impacts (e).

(2b) State Variable Measure: The state variable measures variables outside of the organizational boarders. The inclusion of parnerships and supply chains relationships shows that the ASIS standard explicitly includes the measurement and modeling of external conditions. However, no concrete definition for a state variable is provided. In the same way as the (2a) performance measures have to be defined by the organization itself, it has to be done for the state variable measures. Concerning risks, especially *external risks* according to Kaplan and Mikes definition, can be included as external state variable [2012; 2013]. In concert with the *level of resilience (A.3.1.i)* and *external hazards*, the level of external risks on internal assets and processes can be modeled as state variable.[8]

(3a) Deviation: The deviation in the sense of the CMF is not stated in the ASIS standard. The analysis of the (2) measure-activity and the related information entities called (2a) performance measure and (2b) state variable measure make clear that there exist two types of deviation. The first type is the *level of risk deviation* that indicates the deviation between the current *level of risks (A.4.3.3.g)* and the *objectives and targets for risk prevention, reduction and mitigation (4.3.3.a)* defined in (2a) objectives. The second type is the *level of resilience deviation* that indicates the deviation between the current *level of resilience (A.4.3.3.g)* and the planned *objectives and targets for resilience enhancement (4.3.3.b)* as well as *objectives and targets for financial-, operational- and business-continuity (4.3.3.c)*.

(4a) Closed Loop Control Input: Derived from the goal of the closed loop control cycle, namely the improvement of business performance and resilience, the input is a prescribed practice, action or measure that will modify levels of risk or resilience. Due to a missing definition we call it *corrective closed loop risk control* and *corrective closed loop resilience control*.

(4b) Open Loop Control Input In the same manner, the definition was derived above in (4a), we define the necessary control input as *corrective open loop risk control* and *corrective open loop resilience control*.

(5a) Closed Loop Control Input: The result of the second order closed loop control cycle provides input for the planning system. This input is based on observations of the business and control system as well as involved activities and information flow. The input is not defined in ASIS, but we call it *adaptive closed loop risk management control* and *adaptive closed loop resilience management control*.

[8] Is must be annotated, that the actual realization of a risk as risk event can be compared to the term crisis or hazard. However, there exist crises that can not be anticipated. Therefore, a distinct entity-type for a crisis is provided. This shows that, besides the clear distinctions, there exists as strong interrelation between risk and resilience management that will be explored in detail in Section 5.3.

(5b) Open Loop Control Input: As in (5a), the input for the planning system is not defined in ASIS. We call it *adaptive open loop risk management control* and *adaptive open loop resilience management control* .

(6 Input) Process Supervision Input: The input for the supervision is the organizational *resilience management policy (4.2)*, the *resilience management objectives (4.3.3)* and the observable business processes.

(6 Output) Process Supervision Output: The output is not explicitly defined in the standard, but can clearly be derived as *operational control input for business processes* that aims to increase reliability, resilience of business processess as well as the safety of people and protection of property (related with the supervised business process) in the case of an disruptive incident. The process supervision output can be seen as enforcement rules on the business process level that shall guarantee the *continual improvement (4.6.5)* on the basic process level.

(7 Input) Control Supervision Input: *Results of previous audits (4.5.5)*, *corrective and preventive actions (4.5.3)* taken before, *organizational resilience management system,* programs, processes, procedures (4.5.2.1)*,* legal and regulatory requirements (4.5.2.1)*. As input for the* control of documents (4.4.5)*, all elements that are part of the resilience management* system documentation (4.4.4) *are used to supervise the control system.*

(7 Output) Control Supervision Output: *Records of evaluations (4.5.2.1)*, *post-exercise report (4.5.2.2.d)* including outcomes, recommendations; *records as results of corrective and preventive actions taken (4.5.3.d)*, *documentation (4.4.4)* are updated and provided as enforcement input for the control system what incorporates the *continual improvement (4.6.5)* of the control system.

(8 Input) System Supervision Input: *Review input (4.6.2)* including (a) audit/review-results, (b) feedback from parties, (c) techniques, products, procedures, (d) status of preventive and corrective actions, (e) results of exercise and testing, vulnerabilities or threats not adequately addressed previously, (g) results from effectiveness measurements, (h) follow-up action from previous management reviews, (i) any changes that could affect the organizational resilience management system, (j) adequacy of policy and objectives, (k) recommendations for improvement are used as input for system supervision.

(8 Output) System Supervision: *Review output (4.6.3)* includes the (a) improvement of resilience management system effectiveness, (b) update of risk assessment, impact analysis, incident preparedness, response plans, (c) modification of procedures and controls that effect risks, (d) resource-needs are provided as feedback and enforcement rules for the whole organizational resilience management system. This input generation is the implementation of *continual improvement (4.6.5)* on the organizational resilience management system level.

5.2.3 Evaluation of the Framework

The ASIS standard lays the focus on *prevention, preparedness and response (4.4.7)*. This includes the management of risk and resilience. *Risk* can be treated by reducing the likelihood of a potential risk event and by reducing the impact of potential risks-events. The minimization of likelihood is a core activity of risk management, whereas, the reduction of hazardous impacts involves risk management, business continuity management and emergency planning. The main focus of business continuity management is the preparedness of systems, assets and processes. The focus of emergency or crisis management is the response to a crisis. The encompassing resilience management of ASIS includes different management cycles, as defined in the Cybernetic Management Framework. The implementation of these management cycles is evaluated below.

Open and Closed Loop Resilience Management

The *closed loop control cycle* of the ASIS standard focuses on first order *control and improvement of the internal business system*. The target is to achieve business goals by securing all types of assets. The closed loop cycle measures and evaluates the *risks on business objectives* and the *resilience-level of assets in relation with distinct risks*. It appears that the management of risks and resilience is strongly interlinked by the interrelation between distinct risks and the related resilience level of assets.

The *open loop control cycle* focuses on the observation of events and indicators outside of the organization. This is especially interesting for the envisioning of external risks and hazards. The internal reaction to external change, observed and modeled as state variable, can either be a risk management or a resilience management activity, as described in the paragraph above.

First and Second Order Learning

First order learning allows to improve business processes by *analyzing the business system, the related business environment* and providing new control input. The business system is controlled by the (2a) performance measure on risk on resilience and the environment is modeled as (2b) state variable. The core process of first order learning happens in (4) corrective-act.

Second order learning allows the organization to adapt the whole resilience management system or parts of it like risk measures or resilience management processes. The main action of second order learning is conducted in (5) adaptive act-activity. In Schwaiger's sense the validity of measures can be evaluated and renewed [2012]. If the measures for the *level of risk* or the *level of resilience* turn out to be inaccurate, the measures or even whole control cycles can be adapted. This adaptive learning process is the main implementation of the continual improvement that is one of ASIS' main goals.

Pro- and Reactive Resilience Management

Reactive resilience management happens mainly in the emergency *response (4.4.7)* and partly in *prevention and preparedness (4.4.7)*. The prevention of risks or asset-vulnerability can be a

reactive action triggered by historical performance or environment data that has been captured in the past business periods.

Proactive resilience management is conducted in *preparedness and response (4.4.7)* where risks and vulnerability of assets are envisioned and proactive measures are initialized to prevent negative impacts on the achievement of business goals in the future. The ASIS standard semantically defines these proactive actions, however the semantic meaning of proactivity in this context denotes an envisioning of which actions will be necessary to prevent and prepare crises. This envisioning bases on realized performance measures, whereas proactivity in Schwaiger's sense bases on the comparison of planned objectives with stochastically forecasted performance measures. This stochastic control theory can definitely be included in the ASIS standard, but is not part of ASIS. As consequence we see that the heart of ASIS activities base on *Schwaiger's concept of reactivity*.

KEY FINDINGS

- The core goal of ASIS is to ensure the achievement of business goals by reducing risk on and increasing resilience of assets.
- The risk management part of ASIS has, in the same manner as ISO 31000, the theoretical foundation to be implemented as holistic risk and resilience management system.
- ASIS combines classic risk management with the aspects of business continuity, security and emergency management.
- It is defined in a generic way that allows to integrate other related standards that guide on how to implement resilience management sub-processes like business continuity and security management.
- There is a clear distinction between risks, risk events, hazard and crises. However, crises are potential risks realized as actual risk events. The seamless integration of these semantic definitions and concrete management processes is still hindered by the theoretical and scientific separation of the involved management and research domains.
- Cultural aspects of resilience are part of the ASIS standard but they lack a guidance on how to introduce a climate that promotes employees to communicate risks and potential hazards actively.

ANSWER TO RESEARCH QUESTION 4

1.1 Which activities, information and information flow shall a cybernetic management framework for resilience management include?

- *See Figures 5.3, 5.4 and related description.*

5.3 Comparison of Risk and Resilience Management

As the evaluation of the developed risk and the resilience management frameworks, the comparison of both bases on the core elements of Schwaiger's Cybernetic Management Framework, namely, the different types of control cycles. The following paragraphs describe similarities of and differences between both developed frameworks.

Open and Closed Loop Management

The *closed loop management cycles* of both, ASIS and ISO 31000, focus on the achievement of business goals by controlling and improving the internal business system in a way that increases the probability of surviving risk realizations. In both standards this can be arrived by *decreasing the probability of risk events* or by *decreasing the impact of potential risk events*. What ASIS adds to the ISO 31000 functionality is the concept of *responding to a realized event or crisis*. This means the focus of ISO 31000 risk management lies on the prevention, whereas ASIS does the same but adds *response activities*. Response activities include crisis management and all activities that help the organization to *recover from an impact*. The realization is done by adding a strong *focus on assets* (information, technology, human, infrastructural). ASIS defines not only risks on assets but also resilience and the potential to recover from a crisis in dependence of different assets.

The *open loop management cycles* of both, ASIS and ISO 31000, observe organization-*external environment like stakeholders, business environment or critical events*. In ISO 31000 there are no details provided on this management cycle. In the ASIS standard some more information can be found concerning the management of external supply chains or the observation of and reaction to external hazards. Again, by the introduction of assets the interlink between the internal and external business system can for example be strengthened by *managing the asset-dependency on external suppliers*.

First and Second Order Learning

First order learning is a central part of risk and resilience management. The first order management of business performance, aiming to finally increase the probability of achieving business goals, is part of both management fields. The adaption of business operation as reaction to internal or external changes is also included in both approaches. *Second order learning* allows to reflect the whole planning and control system as well as the first order learning cycle. Both, risk and resilience management use the (5) adaptive action to review the planning and control

system with regard to changes in the environment or with in the own organization. It can be used to restructure whole management cycles or to check the validity of measures used in the first order control cycle. The difference between risk and resilience management concerning first and second order learning is the following: In risk management learning can only be done by reflecting preventive actions that happen before a risk realizes, whereas, in resilience management learning can also be done by reflecting the corrective actions that are conducted during or after a crisis.

Pro- and Reactive Management

The *reactive management cycle* is firstly used to react to internal performance-changes, risk or resilience measures and secondly to react to changes in the organization-external environment. This is conducted in risk and resilience management, again with the restriction that risk management does not include crisis or business continuity management.

The term *proactive management* is used in the ASIS and ISO 31000 standards and means the proactive reduction of risk or increasing of resilience by reacting to already realized business performance or measured changes in the external business environment. In the sense of Schwaiger's definition of proactive management, as stochastic forecasting by comparing planned values to forecasted values, is neither conducted in the ASIS nor in the ISO 31000 standard. However, it can be included in both modeled Cybernetic Management Frameworks in the same way Schwaiger does in his work on the COSO Enterprise Risks Management Framework [2012].

5.3.1 Key Findings

The comparison of the developed Cybernetic Risk Management Framework and the developed Cybernetic Resilience Management Framework above reveals a broad field of common management activities and related information flow.

The major difference between risk and resilience management that arose during the evaluation is that risk management focuses on the prevention of risk and the minimization of risk impact, whereas resilience management does the same but adds the focus of recovery from realized risks as crisis. This fact can be found on each of the analyzed management cycles (the open, closed, first-order, second-order, reactive and proactive-management cycles).

The additional management field of recovery includes crisis management and business continuity management. *Business Continuity Management* includes the prevention, preparedness, response and recovery phases of resilience management and has therefore a strong overlapping with risk and crisis management. Risk and crisis management deal with distinct phases of resilience management and resilience management as whole includes all the depicted management fields and some, up to now, not clearly semantically defined actions that are described in the Cybernetic Resilience Management Framework. A visualization of the different management domains that are part of the resilience management life cycle as well as the variation of the firm's key-performance-indicators (KPI) is visualized in Figure 5.5.[9]

[9]Figure 5.5 shows one possible course of key-performance-indicators (KPI) before, during and after a crisis. The actual types of measured KPI depends on the type of observed enterprise and branch of business (compare [McManus, 2008; Stephenson, 2010]).

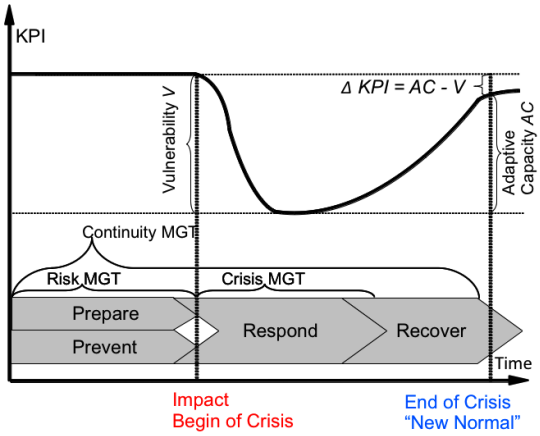

Figure 5.5: The Phases of Resilience Management

Comparing the elicited management fields that are part of *resilience management*, namely *risk management, crisis management* and *business continuity* management, with existing functional models we can find strong support for the developed point of view: Gibson and Tarrant present an *Integrated Functional Model of Resilience Management* that strongly overlaps with the results of the evaluation above [2010]. The Integrated Functional Model includes the *emergence, crisis, business-continuity, risk,* and *security management areas* as visualized in Figure 5.6.

Figure 5.6: Integrated Functional Model of Resilience Management

In accordance with Gibson and Tarrant [2010].

Gibson's and Tarrant's explanations on the distinct management functions within resilience management strongly support the evaluation above. They additionally adduce the security management area which is not part of ISO 31000 or ASIS. The term emergency management is

illustrated by them as separate management area, although it can be sensibly included as part of crisis management.

KEY FINDINGS

- Risk management focuses on the prevention of and preparedness for risk events.
- Resilience management does the same, but adds the functionality of recovery management by means of risk and business continuity management.
- Risks management is a real subset of resilience management.
- Risk and resilience management use first order learning to improve business performance and to reach business goals.
- Risk and resilience management use second order learning to improve the whole planning and control system cycles.
- Proactive management in the sense of stochastic forecasting and control is not part of ISO 31000 or ASIS but can easily be included by means of the developed frameworks.

ANSWER TO RESEARCH QUESTION 5

1.1 What is the difference between risk management and resilience management concerning activities, information flow and cybernetic management levels?

- *Risk management focuses on the phases before a crisis occurs, namely on prevention of and preparedness for risks. Resilience management does the same but adds the aspect of successfully recovering from a realized risk by means of crisis and continuity management. Therefore, risk management activities and information flows are a real subset of resilience management activities.*
- *All cybernetic management cycles exist in both, risk and resilience management. However, in resilience management has a stronger focus on the management of external events, by adding a dependency-relation between internal assets and external conditions or suppliers.*

5.4 Integrated Enterprise Risk and Resilience Management Framework

The developed frameworks for risk management in Section 5.1 and for resilience management in Section 5.2 can by applied to any organizational entity like a business unit for example. To

take the frameworks to the enterprise level, some extensions are required. At the enterprise level a cybernetic management framework must be capable of modeling all organizational subsystems and the included control cycles. A classical enterprise hierarchy consists of several subsidiaries, each subsidiary is made up by several business units, each business unit includes several divisions. The development of an enterprise risk and resilience management framework requires the steps illustrated in the following sections.

5.4.1 Integration of the CMF and the MSC into a Recursive Cybernetic Management Model

In Section 2.1 two different models for planning and control were introduced. The first model, Schwaiger's *Cybernetic Management Framework (CMF)*, was used as core methodology for modeling the ISO 31000 Risk Management Standard and the ASIS Organizational Resilience Management Standard. The second model, Schwaninger's *General Model of Systemic Control (MSC)*, constitutes the heart of the famous St. Gallener Management Model and is one of the most diffused approaches for enterprise management. Before the elaborated *Cybernetic Risk Management Framework* and the *Cybernetic Resilience Management Framework* can be extended to an enterprise-wide management system, an integration of Schwaiger's CMF and Schwaninger's MSC has to be conducted.

As depicted on Figure 2.5, the MSC is divided into three distinct management systems: *(1) the Normative Management System, (2) the Strategic Management System* and *(3) the Operational Management System*. The analysis in Section 2.1.2 reveals that each of the three systems has different goals, design parameters and dimensions of organizational fitness. The fact that each of the three management systems sets and pursues its own goals involves the necessity of clear control over these goals. The basic cybernetic approach for setting, pursuing, checking and updating management goals is the PDCA-Cycle. The advanced version of the PDCA-Cycle is Schwaiger's Cybernetic Management Framework where the planning and control cycles run over distinct management levels: *(1) the Planning System* that sets goals, rules and regulations, *(2) the Control System* that measures business performance, within *(3) the Business System* and reacts to deviations in performance or in external environments in a corrective or adaptive way. The output of the Control System acts as control input for the Business System and the Planning System.

These considerations point out that an integration of the MSC and the CMF must be constituted the following way: Each of the three subsystems of the MSC, (1) the Normative, (2) the Strategic and (3) the Operative Management System, must consist of an own CMF. A whole MSC must therefore involve three distinct CMFs, one on each vertically separated management level. At the first sight, this might seem likely to introduce unnecessary complexity, however, the logical arguments that (a) planning, performing, measuring and reacting is indispensable for a serious management system and that (b) the measurement of external and internal variables as well as the re- and proactive management are crucial for business success in modern organizations implicates the proposed integration-concept of the MSC and the CMF.

A further aspect of the integration is hierarchy of control. The Normative Management System must govern the Strategic Management System and the Strategic Management System

has to govern the Operational Management System. The question that arises at this point is "How must the three management systems be interconnected, so that a real governance including *control in the large* and *control in the small* can be accomplished?" The only answer that allows to carry out the enforcement rules on the hierarchically lower system, is when the lower system is part of the higher system. This can be designed by making the lower system a subsystem of the higher system. Following this design, the Operational Management System must be a subsystem of the Strategic Management System and the Strategic Management System must be a subsystem of the Normative Management System. The governance concept that allows to plan and provide rules for the subsystem can be implemented by integrating the subsystem into the Operative System of the distinct Management Level. This reveals that the integration of the CMF and the MSC ends up in the necessity of a *Recursive Cybernetic Management Model (RCMM)*. The basic version of the model is visualized on Figure 5.7. This figure visualizes the core elements of the CMF and the MSC as well as the matching of the two frameworks and the *recursion principle*.

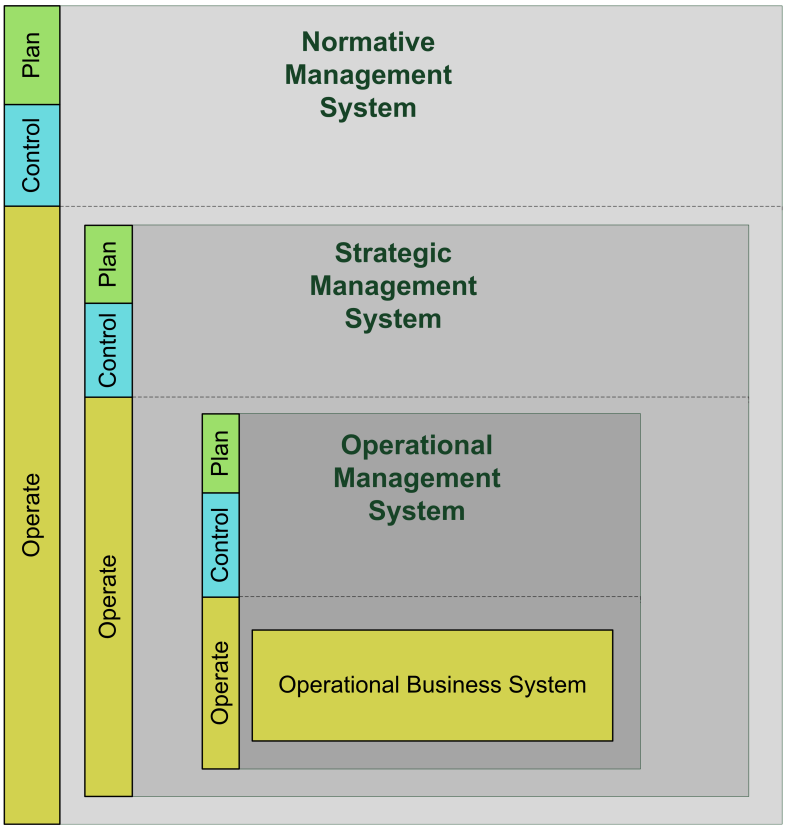

Figure 5.7: The Recursive Cybernetic Management Model (CRMM)

Up to now, the elaborated *Recursive Cybernetic Management Model* can be applied to any entity of an organization. To raise the concept to the enterprise level, a further step of recursion is necessary. To take this step, a look at a concrete implementation of the Recursive Cybernetic

Management Framework within an organization is necessary. Assuming that in a concrete organization, the RCMM is used to manage one business unit of the organization. This business unit is part of a subsidiary and the subsidiary is again part of the main company. This enlarges the *concept of recursion* from within the RCMM to the *organizational context*. The conceptual design of the RCMM includes the whole RCMM of the business unit as subsystem of the Operative Level of the Operational Management System within the subsidiary's RCMM. This *external recursion* is visualized on Figure 5.8. The recursion of the Normative, Strategic and Operative Management Systems over the hierarchy of an enterprise has been described by Schwaninger, who combines the MSC and Viable System Model[10] [2000]:

> According to the *Viable System Model [VSM]*, all three levels of management - operative, strategic and normative - are distributed functions, with aspects such as control, intelligence, and ethos being properties of the system as a whole, and inherent in all levels of recursion. This contradicts the often-repeated comments that "vision is the concern of the entrepreneur," or "strategy is the duty of the board of directors." Vision is a function of the meta-system: to be precise, it is one of the functions of the normative management of every viable unit. Strategic thinking is necessary even in the smallest units, if such units are conceived as viable wholes. [Schwaninger, 2000, p.225]

The new developed *Recursive Cybernetic Management Model (RCMM)* is generic in its approach, as Schwaiger's CMF is, and extends his model to enterprise management. What is still missing in the visualization on Figure 5.7 is the monitoring of external environments. The CMF includes the observation of external changes in the business environment and models it as *state variable*. This state variable must also be part of each CMF within the new RCMM. This means that the Normative Management System has an own state variable for observing and modeling changes in the normative business environment. This environmental changes for the Normative Management System can for example be legislative changes concerning the regulation of the performance based incentives for the top management of european banks. In the same way, the Strategic Management System has a own environment. For example, the competitive market including attributes like the market attractiveness, the number of competitors and their strengths. The same way the RCMMs are nested recursively, the environments are, as Beer proposed in a similar way for the Viable System Model. The inclusion of the recursive environments is visualized on Figure 5.8.[11]

Figure 5.8 is an encompassing visualization of the *Recursive Cybernetic Management Model* including the distinct environments of each management subsystem which are nested in the same way the management systems are themselves.

[10] Beer developed the *Viable System Model (VSM)* as cybernetic model consisting of recursively nested viable systems that constitute a bigger system. Schwaninger refers to this recursion in the VSM but does not visualize that the system at recursion level *i+1* is part of the system at recursion level *i*. The goal of the higher system is always to control the systems at lower levels, therefore deeper recursion levels must always be part of higher one as visualized in the Figure 5.7

[11] The hand-drawn illustration of the environments in the style of Beer's Viable System Model is an intended way to show the conformity in concept.

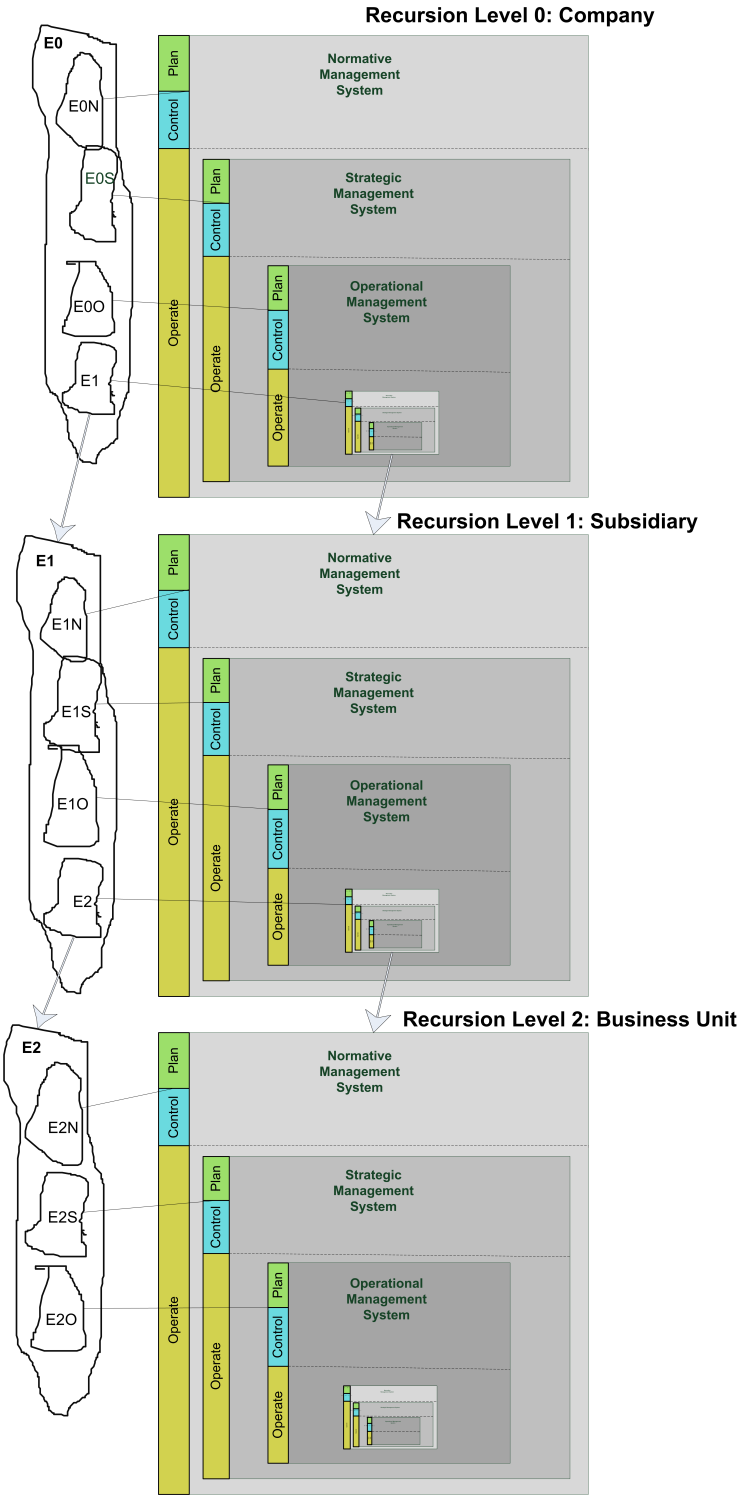

Figure 5.8: The Recursive Cybernetic Management Model and its Environments

With this step, the integration of the CMF and the MSC into the RCMM is completed, as the necessary system-structure, the related environments and the management control cycles are defined at the requested high level that fits as meta-model. In the next step the developed *Cybernetic Risks Management Framework* and the *Cybernetic Resilience Management Framework* can be combined to an *Enterprise Risk and Resilience Management Meta-Framework* by using the new *RCMM*.

5.4.2 Enterprise Risk and Resilience Management as Recursive Cybernetic Management Model

Following the new Recursive Cybernetic Management Model, an Enterprise Risk and Resilience Management Meta-Framework must also contain the following subsystems hierarchically ordered: (1) the Normative Resilience Management System (2) the Strategic Resilience Management System (3) the Operational Resilience Management System and the (4) Business System. Each of those systems is constituted by 3 subsystems the (a) Planning System (b) Control System and (c) Operative System. Before explaining the details of the new integrated system, the core operational management subpart is elaborated.

Structuring the Enterprise Risk and Resilience Management Meta-Framework

The operational resilience management system includes the core resilience activities, described in the ASIS and ISO 31000 standards. Therefore, the elaboration of the enterprise-wide risk and resilience management meta-framework start with this system. In Section 5.3 the developed *Cybernetic Risk Management Framework* and the *Cybernetic Resilience Management Framework* are compared and evaluated. The scientific result of this section was, that risk management is a real subset of resilience management and *resilience management extends risk management* with *crisis management* and *business continuity management*. Following these research results, the operational resilience management level must include operational (1) risk, (2) crisis and (3) business continuity management. The detailed design of the management levels is described in the following paragraphs and figures.

The Operative Level of the Normative Resilience Management System includes all other subsystems, as they are driven by the Normative Resilience Management System. The Operative Level of the Strategic Resilience Management System includes in it's Operational Level the Risk Management Subsystem, the Crisis Management Subsystem and the Business Continuity Subsystem as well as the Business System. The Operational Level of the Risk, Crisis and Business Continuity Management Subsystems includes only the Business System. This makes clear that the hierarchical *Enterprise Resilience Management Meta-Framework*[12] is a system that is recursively constituted by subsystems where all subsystems are part of the higher systems and by the recursive definition of the enterprise planning and control cycles.

[12] In the course of the research process on integrated risk and resilience management, it became obvious that risk management is one of the sub-management systems of enterprise resilience management. Therefore, the planned name of *Integrated Enterprise Risk and Resilience Management Meta-Framework*" is transferred into *Enterprise Resilience Management Meta-Model*. This meta-framework includes risk management as subsystem and takes the necessary risk management activities to the enterprise level.

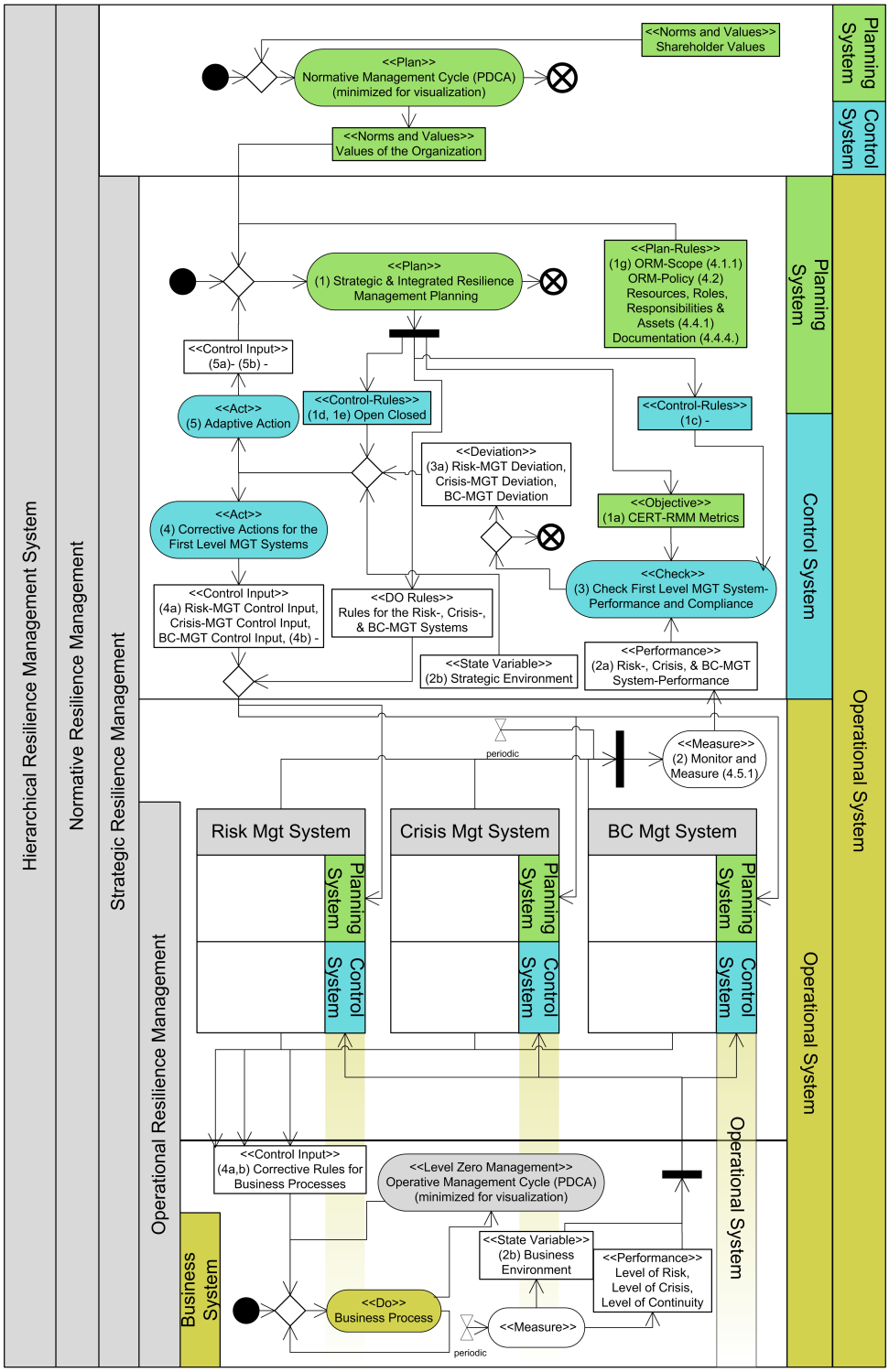

Figure 5.9: Enterprise Resilience Management Meta-Framework (ERM-MF)

The new developed *Enterprise Resilience Management Meta-Framework (ERM-MF)*[13] provides a *cybernetic steering meta-model*, what was the main goal of this thesis. To guarantee that the operational resilience management processes are conducted in an effective and efficient way, some kind of quality assurance for the new developed meta-framework would be useful. ISO [2009, p. 8] proposes to integrate management maturity aspects to enterprise risk management. The same can be done for the new ERM-MF to guarantee the *operational management process quality*. The next section includes the aspect of management process capability into the ERM-MF.

5.4.3 Including Process Capability Metrics in the Enterprise Resilience Management Meta-Framework

In the ERM-MF the Operational Management Level contains three Cybernetic Management Frameworks as subsystems. These three subsystems are the *Operational Risk, Business Continuity* and *Crisis Management Systems*. To measure the performance and process quality of the three Operational Management Systems, a process capability management for all resilience management activities within the three systems will be introduced.

The Operational Risk Management System can either base on the ISO 31000 Standard, as modeled in Section 5.1 or on the ASIS standard, modeled in Section 5.2. The Operational Business Continuity Management System and the Operational Crisis Management System base on the relevant parts of the ASIS standard modeled in Section 5.2 . Therefore, all activities that are used on the Operational Levels in the ERM-MF are part of ASIS or ISO 31000 and can be looked up, if details on activities or information flow are required.

So, if the *process capability of the Operational Resilience Management Systems* shall be measured, all the activities of the ASIS and ISO 31000 standard that were modeled in the Sections 5.1 and 5.2 have to measured and evaluated. As basis for the process capability analysis the *CERT Operational Resilience Management Model (CERT-RMM)* [Caralli et al., 2010a,b,c] will be used. The main goal of this model is to provide goals and metrics to improve several hundred operational resilience management activities. Therefore, the process capability approach of this model is perfect fitting for being included in the developed ERM-MF. The CERT-RMM was designed in a high level way that allows the combination with other management standards, for example, risk management or security management standards.

The CERT-RMM is divided into four main management areas, namely *engineering, operations, enterprise management,* and *process management*. These four management areas include 26 process areas, which include 94 specific resilience goals and 251 specific practices that support the achievement of the specific goals and therewith the process capability of the related resilience management process area.

Through an *extensive content analysis* of the CERT-RMM most relevant process areas for the integration into the ERM-MF were selected. These process areas are listed in Table 5.1. Within these process areas all specific practices were compared to the ASIS and ISO 31000

[13]The new developed meta-framework does not include the word “risk” as semantic element of definition, as previous elaborations have showed that risk management is a functional subset of the resilience management domain. Nevertheless, the main aim of integrated enterprise risk and resilience management is still prevailing in the new meta-framework.

Engineering		**Operations**	
ADM	Assets Definition and Management	IMC	Incident Management and Control
CTRL	Controls Management	VAR	Vulnerability Analysis and Resolution
SC	Service Continuity		
Enterprise Management		**Process Management**	
COMM	Communications	MON	Monitoring
COMP	Compliance		
OTA	Organizational Training and Awareness		
RISK	Risk Management		

Table 5.1: Selection of CERT-RMM Process Areas that Comply with the ASIS and ISO 31000 Management Activities

management activities to elicit measures that can be used for the ERM-MF. As result, a list of appropriate measures was developed and is included in Appendix A.2 and A.3. All metrics listed, are measured and modeled as *(2a) Operational Management System Performance*. All measures are either part of the *Operational (1) Risk, (2) Business Continuity* or *(3) Crisis Management Performance* entities in Figure 5.9.

Whenever an enterprise management team wants to introduce the Enterprise Resilience Management Meta-Framework, it can decide which risk and resilience management activities are crucial for the business success and look up the activities in the appendix to find out which metrics can be used for the operational risk, business continuity and crisis management. The details on the fitting metrics can be looked up in Allen and Curtis [2011]. Support for the measurement process can be found in Allen and Davis [2010].

This part of the ERM-MF follows the main concept of the thesis, namely, the allocation of high level cybernetic models that can be used by any organization. During the integration of the CERT-RMM process metric, ASIS released a own resilience maturity model. This can be seen as confirmation of the approach that was chosen for this section of the thesis by one of the most respectable standardization institutions worldwide. The advantage of the CERT-RMM metrics is that they are freely available for anyone, whereas the *ASIS Resilience Maturity Model* is only available at charge.

The summarizing view on the ERM-MF shows that risks, resilience of assets and the business continuity performance can be measured on the Operational Resilience Management Level in Figure 5.9. The details on this operational management can be found in Sections 5.1 on Cybernetic Risk Management and 5.2 on Cybernetic Resilience Management. The maturity of the operational risk, crisis and business continuity management systems itself can be evaluated by the introduced CERT-RMM metrics in the Strategic Resilience Management System.

Finally, the necessary business processes including risks and assets can be measured and evaluated by the two Cybernetic Frameworks developed in Sections 5.1 and 5.2, but also the Operational Resilience Management System itself, including Risk, Business Continuity and Crisis Management, can be evaluated by the new introduced CERT-RMM metrics. This shows that *the introduction of the additional cybernetic levels from the MSC was necessary to reach the*

final goal of the ERM-MF - a mature and integrated enterprise risk and resilience management system.

5.4.4 Key Findings

The integration of risk and resilience management ended up in the *Enterprise Resilience Management Meta-Framework (ERM-MF)*. This framework bases on the new developed *Recursive Cybernetic Management Model (RCMM)* that originated from the integration of the *Cybernetic Management Framework (CMF)* and the *Model of Systemic Control (MSC)*.

Considering all research findings of the previous sections and chapters, a distinct picture of integrated enterprise risk and resilience management emerges. The core of the concept constitute the assets of the organization as well as the processes that use and combine the assets and the services that assemble the business processes as direct added customer or product value. These aspects embody the business system of the organization.

The *Operational Resilience Management System* is vertically structured as explained above. It includes (1) Risk, (2) Crisis, (3) Business Continuity and (4) Process Management that make up the functional management domains required for capable resilience management. Process management bases on the process capability metrics introduced above.

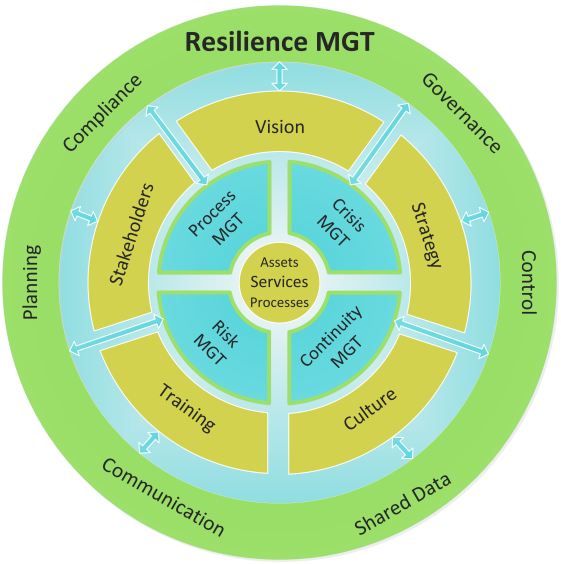

Figure 5.10: A Composite Model of Enterprise Resilience Management (CM-ERM)

The *Strategic Resilience Management System* coordinates and steers the operational resilience management activities by using the vision of the *Normative Resilience Management System*, involving stakeholders, training and activating personnel by developing the required organizational culture and resilience management strategy. Management views within the strategic resilience management include the aspects of planning and control, governance, compliance, redundant communication channels and data.

As result of all key findings, a *Composite Model of Enterprise Resilience Management (CM-ERM)* evolved. This model is shown of Figure 5.10 and illustrates the necessary components, functionalities and meta-structure of enterprise resilience management in a very abstract way.

KEY FINDINGS

- The General Model of Systemic Control (MSC) and the Generic Cybernetic Management Model (CMF) could be integrated into the new *Recursive Cybernetic Management Model (RCMM)*.
- The heart of the RCMM is constituted by the fact that each, the Normative, the Strategic and the Operative Management System of the MSC is constituted by one CMF.
- The RCMM integrates the ideas of recursiveness and distinct environments for each management subsystem from the Viable System Model.
- The RCMM can be applied to any organizational hierarchy, independent from its size and complexity.
- The RCMM could be used to successfully integrate the developed *Cybernetic Risk Management Framework* and the *Cybernetic Resilience Management Framework* into the new *Enterprise Resilience Management Meta-Framework (ERM-MF)*.
- The ERM-MF can, in the same way as the general RCMM, be applied to any organization independent of industry, size and organizational structure.
- The ERM-MF uses, at the Strategic Management Level, the process capability metrics of the CERT-RMM to measure the operational resilience management performance within the enterprise entities. This performance metrics can be aggregated horizontally and vertically in the same way risk performance aggregation is conducted.
- The *Composite Model of Enterprise Resilience Management (CM-ERM)* was developed as final result which visualizes all integrated functionalities, components and interactions of enterprise resilience management.

ANSWER TO RESEARCH QUESTION 6

1.1 How can risk management and resilience management be integrated into one cybernetic enterprise management framework?

1 *The integration requires, as first step, the combination of the General Model of Systemic Control (MSC) and the Generic Cybernetic Management Framework (CMF) into the new Recursive Cybernetic Management Model (RCMM), as visualized on Figure 5.8 and explained in Section 5.4.1.*

2 *On the basis of the new RCMM, an Enterprise Resilience Management Meta-Framework (ERM-MF) could be developed, as illustrated on Figure 5.9 and explained in Section 5.4.2.*

CHAPTER 6

Critical Reflection

" The opposite of a correct statement is a false statement. But the opposite of a profound truth may well be another profound truth. "

[Nils Henrik David Bohr, 1885 - 1962.]

Contents

6.1 Evaluation of the Developed Meta-Framework **85**
6.2 Comparison with Related Work **88**
6.3 Discussion of Open Issues **89**
6.4 Conclusion **90**

Abstract This chapter reflects and evaluates the strengths and weaknesses of the used methodology and the developed frameworks. A discussion of open issues and a comparison with related work completes the chapter.

6.1 Evaluation of the Developed Meta-Framework

The Design Science research approach has the goal to provide new theoretical concepts and artifacts that can be implemented as information system to support the fulfillment of organizational resilience indicators. These resilience indicators that have to be fulfilled by organizations to become more resilient have been elaborated by Stephenson [Stephenson, 2010] basing on McManus', Weick's and Suttcliffes work [McManus, 2008; Weick, 1993, 1995, 2001; Weick and Sutcliffe, 2003; Weick et al., 2008; Weick, 2009].

In Table 6.1 the developed *Enterprise Resilience Management Meta-Framework* is evaluated against the indicators for resilience, as planned in the methodological concept in Section 2.3. The evaluation compares core elements of the developed meta-framework to Stephenson's resilience

indicators. The evaluation rates the fulfillment-degree of the related organizational resilience indicators.

Resilience Indicator	Goal Description	Fulfilled	Means of Fulfillment
Adaptive Capacity			
Minimisation of Silo Mentality	Minimisation of divisive social, cultural and behavioral barriers, which are most often manifested as communication barriers creating disjointed, disconnected and detrimental ways of working.	partly	ASIS: Communication and Warning (4.4.3)
Capability & Capacity of Internal Resources	The management and mobilization of the organization's resources to ensure its ability to operate during business as usual, as well as being able to provide the extra capacity required during a crisis.	yes	ASIS: (1g) Resources and Assets (4.4.1), (1) Requirements Identification (4.3.2), (1b) Requirements Identification Rules (4.3.2.a), (1f) Asset Identification Rules (4.3.1.a)
Staff Engagement & Involvement	The engagement and involvement of staff who understand the link between their own work, the organization's resilience, and its long term success. Staff are empowered and use their skills to solve problems.	partly	ASIS: Communication and Warning (4.4.3), Roles and Responsibilities (4.4.1)
Information & Knowledge	Critical information is stored in a number of formats and locations. Staff have access to expert opinions when needed. Roles are shared and staff are trained so that someone will always be able to fill key roles.	hardly	ASIS: Training (4.4.2), Communication (4.4.2)
Leadership, Management & Governance Structures	Strong crisis leadership to provide good management and decision making during times of crisis, as well as continuous evaluation of strategies and work programs against organizational goals.	most	ASIS: Evaluation against organizational goals is done in (7), (8) Supervisory Control. Crisis Leadership depends on the personality of managers, but can be improved by Training (4.4.2).
Innovation & Creativity	Staff are encouraged and rewarded for using their knowledge in novel ways to solve new and existing problems, and for utilizing innovative and creative approaches to developing solutions.	no	Missing in ASIS and ISO 31000.

Resilience Indicator	Goal Description	Fulfilled	Means of Fulfillment
Devolved & Responsive Decision Making	Staff have the appropriate authority to make decisions related to their work and authority is clearly delegated to enable a crisis response. Highly skilled staff are involved, or are able to make, decisions where their specific knowledge adds significant value, or where their involvement will aid implementation.	partly	ASIS: Roles and Responsibilities (4.4.1), Training (4.4.2) ensures highly skilled staff. However, crisis response does always depend on personalities and crisis-types.
Internal & External Situation Monitoring & Reporting	Staff are encouraged to be vigilant about the organization, its performance and potential problems. Staff are rewarded for sharing good and bad news about the organization including early warning signals and these are quickly reported to organizational leaders.	partly	The internal change is measured as (2a) Level of Risk and Resilience in the (2) Measure Activity. External change is modelled as (2a) State Variable. Both are evaluated in (4) Corrective and used in (5) Adaptive Actions. ASIS: Communication and Warning (4.4.3).
Planning			
Planning strategies	The development and evaluation of plans and strategies to manage vulnerabilities in relation to the business environment and its stakeholders.	yes	Plans and Strategies are developed in (1) Plan, evaluated in the (5) Adaptive Act as well as (8) System Supervision and re-planned in (1) Plan of the developed Frameworks.
Participation in Exercises	The participation of staff in simulations to practice response arrangements and validate plans.	yes	Exercises are core part of the (4) Corrective Act in the Cybernetic Resilience Management System.
Proactive Posture	A strategic and behavioral readiness to respond to early warning signals of change in the organization's internal and external environment before they escalate into crisis.	yes	ASIS: The Proactive Management of Risks (A.0) is the heart of the Standard. Roles and Responsibilities of Employees concerning Risk Reporting (4.4.1, A.4.7.g).
Capability & Capacity of External Resources	An understanding of the relationships and resources the organization might need to access from other organizations during a crisis, and planning and management to ensure this access.	yes	ISO 31000: (1) Plan: Establish External Context (2.10) with External Stakeholders (2.13); ASIS: (1) Plan Risk and Impact Analysis (4.3.1.a) including supply-chain and stakeholders and Identify Related Requirements (4.3.2)
Recovery Priorities	An organization wide awareness of the organization's recovery priorities, as well as an understanding of the organization's minimum operating requirements.	yes	ASIS: Recovery, Prevention and Preparedness (4.4.7) includes the prioritization of recovery needs. Asset-Identification Rules (4.3.1.a) guide the entities in eliciting the core assets and recovery priorities.

Table 6.1: Evaluation of the Developed Meta-Framework

The first eight business goals are part of the main goal of increasing organizational adaptive capacity. The last five business goals are part of the main goal of improving the planning quality within an organization[1].

Improving Planning Due to the nature of the developed meta-framework as *planning and control* framework the goal of improving planning is completely fulfilled. The major problem that might arise is the complexity of the meta-framework. It must be ensured, that experts steer the development, implementation and continual improvement of the whole enterprise-wide resilience management system. The management on lower levels, does not necessarily require to understand the whole system and control cycles.

Increasing Adaptive Capacity Adaptive capacity is a system-property that depends on the capability of an organization to react in a dynamic and self-reflected way to internal and external changes. The adaptive capacity can not be improved by simple planning and control, but the developed cybernetic meta-framework includes elements like second order self-reflection, proactive management for anticipating future events, training of personnel and development of decision competencies. All these elements have the potential to increase the adaptive capacity of an enterprise and its employees. However, attributes like innovation, active reporting, responsive decision making are either not part of ASIS and ISO 31000 or can at least not be prescribed in a theoretical way. So, cultural change management must be part of the implementation of the meta-framework within organizations to minimize the revealed deficiencies in flexible adaptivity.

6.2 Comparison with Related Work

Gibson and Tarrant [2010] provide an overview over existing models of organizational resilience management. According to them there exist (1) functional models, (2) attributional models, (3) process models, and (4) composite models.

1. *Functional Models* integrate the different management functions or domains that are necessary to increase organizational resilience. The comparison of the developed *Cybernetic Risk Management Framework* and the *Cybernetic Resilience Management Framework* endet up in such a functional model that is similar to the *Integrated Functional Model* visualized on Figure 5.6.

2. *Attributional Models* explain organizational resilience from the perspective of necessary features of a resilient organization [Gibson and Tarrant, 2010, p. 8]. The attributional view is integrated in the thesis by the *organizational resilience indicators* that were used for the evaluation above that revealed which attributes are satisfied by the developed cybernetic models.

[1] The practical implementation and assessment of the meta-framework as management information system would be beyond the borders of this thesis and can be done in further research projects.

3. *Process Models* base on the assumption that a range of capable organizational processes contribute towards enhanced resilience [Gibson and Tarrant, 2010, p. 9]. The process model view is implemented in the designed frameworks through the strong *process management approach* basing on the CMF, the CERT-RMM resilience metrics, the ASIS and the ISO 31000 process definitions.

4. *Composite Models* try to integrate soft and hard elements of resilience management like processes, resources, infrastructure, technology, information and knowledge and especially emergent leadership [Gibson and Tarrant, 2010, p. 9]. The heart of these models is the resilience management policy and strategy. The developed *Composite Model of Enterprise Resilience Management (CM-ERM)* (Figure 5.10) integrates all the research findings of the thesis into one composite model.

6.2.1 The Added Value of the Developed Steering Model

The developed frameworks integrate all the views above into one enterprise resilience steering model. The top-down-view of the steering model starts with the developed *Composite-Model of Enterprise Resilience Management* (Figure 5.10) that provides an overview over the composite elements of enterprise resilience management and is followed by the functional view provided in the Sections 5.3 and 5.4.2 to make clear which management domains are involved or even necessary for operational resilience management.

The bottum-up approach that provides details on how to implement resilience management processes is constituted by the described processes of the developed *Cybernetic Risk Management Framework* in Section 5.1 and the *Cybernetic Resilience Management Framework* in Section 5.2.

The core added value of the thesis is the integration of bottom-up and top-down approaches by the developed *Enterprise Resilience Management Meta-Framework (ERM-MF)* at Section 5.4.2 and the associated cybernetic sub-models of operational risk and resilience management at Sections 5.1 and 5.2.

6.3 Discussion of Open Issues

The evaluation above has shown that the developed models do fulfill many of the demanded business requirements or indicators of resilient organizations. However, some aspects are not, or at least not completely, covered.

What is missing, are the aspects of *innovation and creativity* that are necessary for responsive problem solving. The developed cybernetic models provide a meta-frame for risk and resilience management. The fostering of creativity and innovation can be implemented in the context of this meta-frame. Techniques and strategic approaches have to be evaluated in order to fit the organization and its culture.

Organizational culture is a further topic of interest that is not covered by a cybernetic model to the necessary extend. The design and implementation of enterprise risk and resilience management does always require the a fitting culture and cultural change management. Research has proven that the political and cultural attention to risk and resilience management is more

important than a theoretically sound management system [Kaplan and Mikes, 2013, p. 8]. The principles of the ISO and ASIS standards include the necessity of an appropriate culture that allows employees to observe risks, to report them and to meet necessary decisions in order to fulfill their roles and responsibilities and to perform strong crisis leadership. Detailled concepts or prescriptions on how to include cultural change management is neither provided in the developed steering model nor in the associated standards. This softer aspect has to be evaluated and included for enterprise that want to implement the developed meta-model.

Resilience business requirements that are only covered to a minimal extend are *communication channels, information technology* and *redundant data-storage*. For the implementation of these elements models on security and business continuity management can be included in the provided steering model. The implementation depends on the requirements of the regarded organization.

The classical approach of planning and control and the one of adaptive capacity seem to be contradictory to some extend. From the cybernetic point of view that was used for this thesis they are not. *Planning and control as first order cybernetics* and *adaptive capacity as second order cybernetics* were included into one meta-framework. The only contradiction that might exist is the one of existing paradigms of thinking and mental models of management, as Hamel and Valikangas [2003, p. 63] approve. O'Reilly and Tushman [2004] depicted this problem under the term of *ambidextrous organizations* where exploration and exploitation are depicted as apparently oppositional ways of managing an enterprise.

6.4 Conclusion

The planned Design Science research process was implemented in the defined way. Business requirements were elicited by extensive literature analysis in terms of resilience indicators. Artefacts were designed including ontologies and Cybernetic Management Frameworks, as well as detailled description of all included sub-artifacts. The final Enterprise Resilience Management Meta-Framework (ERM-MF) was evaluated against the elicited indicators of resilient organizations. The results of the evaluation can be considered when the developed meta-framework will be implemented as management information system in further research projects.

The main aim of the thesis was to develop a steering model for integrated risk and resilience management. The developed meta-framework satisfies the requested constitution of this steering model. Some aspects like cultural change management, the concrete implementation of redundant information-channels and security management are not covered by the developed solution. However, the generic cybernetic approach allows these aspects to be integrated in further research or in concrete implementations.

CHAPTER 7

Summary and Future Research

" I don't know where my expertise is; my expertise is no disciplines. I would recommend to drop disciplinarity wherever one can. Disciplines are an outgrowth of academia. "

[Heinz von Foerster, 1911 - 2002.]

Contents

7.1 Summary **91**
7.2 Future Research **92**

Abstract This chapter provides the final summary of the thesis including the research approach and the main research findings in a very compact manner. On the basis of the research findings, recommendations for further research on the topic of integrated enterprise risk and resilience management are provided.

7.1 Summary

The first results of the thesis are the developed *Cybernetic Risk Management* and the *Cybernetic Resilience Management Frameworks.* As theoretical foundation for the combination of these two designed frameworks into one enterprise management meta-framework, the Model of Systemic Control and the Generic Cybernetic Management Framework were integrated into the new *Recursive Cybernetic Management Model (RCMM)*. Basing on the RCMM, the Cybernetic Risk and the Cybernetic Resilience Management Framework were integrated into one encompassing *Enterprise Resilience Management Meta-Framework (ERM-MF)*. This new meta-framework was combined with capability metrics of the CERT Resilience Management Model.

The result was a *Enterprise Resilience Management Meta-Framework* that is capable of measuring business risks and resilience of assets, as well as the operational resilience management process performance.

An additional result is the *Composite Model of Enterprise Resilience Management (CM-ERM)* that combines all research findings of the thesis into one abstract model. The model goes along with existing ones, but adds several new aspects of enterprise resilience management.

The chosen *Design Science Methodology* turned out to be a suitable approach to reach the research goals of the thesis. The most relevant business requirements for the improvement of organizational resilience could be elicited and the required artifacts were developed in forms of Cybernetic Management Frameworks and object-ontologies. The developed frameworks could be evaluated against the business requirements what brought to light that the designed artifacts are suitable to fulfill all business requirements dealing with planning aspects and to fulfill at least to a predominant extend of the business requirements concerning the adaptive capacity of organizations.

The added value for the industrial management community, requested by the Design Science methodology, was generated by the provision of encompassing artifacts and steering-models that can be implemented as risk and resilience management information system in further research projects. Not only, that the generated models can be implemented, but even without an implementation, they can be used as systemic management model for the top management of enterprises that desire to improve the resilience of their enterprises.

7.2 Future Research

To evaluate the designed artifacts and management models they should be *implemented as management information system*. The implementation can be tested under real business life circumstances to approve whether the stated benefit for the industrial community complies with the theoretically elaborated one.

A further research topic of interest is the one of combining adaptive capacity with systemic planning frameworks. It should be evaluated, how a flexible reaction to internal and external changes can be converted in the Cybernetic Management Framework (CMF). The second order learning within the CMF incorporates this topic, but it has to be evaluated, how this can be accomplished within complex organizations and information systems. It will be of special interest, how organizations can build information technology structures that can keep pace with the adaptive cycles of organizations [Gunderson et al., 2009]. The research topic of the *ambidextrous organization* [O'Reilly and Tushman, 2004] does also deal with the problem of balancing planning and exploring existing methods versus innovation and exploitation of completely new business and management models.

A softer aspect that could not be solved in the context of this thesis is the one of managing organizational culture in a way that promotes the necessary involvement and empowerment of employees in resilience management, to improve knowledge management related with organizational resilience and to improve the adaptive capacity of the organization. To improve the management of external events, Sheffi's approach of Resilience Engineering, that focuses on the

management of the external supply chain, should be evaluated and integrated into the developed *Enterprise Resilience Management Meta-Framework (ERM-MF)*.

Organizational resilience does always depend on the resilience of people and the resilience information systems. Existing research on how the resilience of individuals can be improved might be included in the Enterprise Resilience Management Meta-Framework on the level of operational personnel development. Last but not least, a clear interface to information system resilience and security management shall be developed to encompass all relevant resilience management domains.

Bibliography

Julia H. Allen and Pamela D. Curtis. Measures for managing operational resilience. Technical report, Software Engineering Institute (SEI), Carnegie Mellon University, 2011. URL www.cert.org/archive/pdf/11tr019.pdf. (Visited on 2013-04-09).

Julia H. Allen and Noopur Davis. Measuring operational resilience using the cert resilience management model. Technical report, Software Engineering Institut (SEI), Carnegie Mellon University, 2010. URL www.cert.org/archive/pdf/10tn030.pdf. (Visited on 2013-04-09).

Robert N. Anthony. Planning and control systems: A framework for analysis. Technical report, Harvard University Graduate School of Business Administration, Cambridge, 1965.

Chris Argyris. Double loop learning in organizations. *Harvard Business Review*, 55(5):115–126, 1977. URL http://hbr.org/1977/09/double-loop-learning-in-organizations/. (Visited on 2013-05-15).

Kenneth Arrow. Control in large organization. *Management Science*, 10:397–408, 1964. URL http://www.jstor.org/stable/2627417. (Visited on 2013-06-16).

Simon Ashby, Tommaso Palermo, and Michael Power. Risk culture in financial organisations: An interim report. Technical report, London School of Economics and Political Science, 2012. URL http://www2.lse.ac.uk/researchAndExpertise/units/CARR/pdf/Risk-culture-interim-report.pdf. (Visited on 2013-06-10).

BCBS. International convergence of capital measurement and capital standards. *Basel Comittee on Banking Supervision*, 2006. URL http://www.bis.org/publ/bcbs128.pdf. (Visited on 2013-06-25).

BCBS. Basel iii: A global regulatory framework for more resilient banks and banking systems. *Basel Committee on Banking Supervision*, 2010. URL http://www.bis.org/publ/bcbs189.pdf. (Visited on 2013-06-25).

Stafford Beer. *Kybernetische Führungslehre*. Herder & Herder, 1972. URL http://books.google.at/books?id=p7K6NwAACAAJ. (Visited on 2012-12-09).

Ran Bhamra, Samir Dani, and Kevin Burnad. Resilience: the concepts, a literature review and future directions. *International Journal of Production Research*, 49:5375–5393, 2011. DOI 10.1080/00207543.2011.563826.

Dennis Blass. Organizational resilience: Security, preparedness, and continuity management systems - requirements with guidance for use asis spc 1-2009. Technical report, ANSI, 2010. URL http://www.asisonline.org/guidelines/ASIS_SPC.1-2009_Item_No._1842.pdf. (Visited on 2012-12-09).

K. Boulding. General systems theory - the skeleton of science. *Management Science*, 2:197–208, 1956.

Richard A. Caralli, Julia H. Allen, Pamela D. Curtis, David W White, and Lisa R. Young. The cert resilience management model - improving operational resilience. Technical report, Software Engineering Institute (SEI), Carnegie Mellon University, 2010a. URL www.cert.org/archive/pdf/10tr012.pdf. (Visited on 2013-04-10).

Richard A. Caralli, Julia H. Allen, Pamela D. Curtis, David W. White, and Lisa R. Young. The cert resilience management model - process areas, generic goals and practices, and glossary. Technical report, Software Engineering Institute at the Carnegie Mellon University, 2010b. URL http://www.cert.org/resilience/download/CERT-RMM_v1.0.pdf. (Visited on 2012-12-09).

Richard A. Caralli, Julia H. Allen, Pamela D. Curtis, David W. White, and Lisa R. Young. Improving operational resilience processes: The cert resilience management model. In *Social Computing (SocialCom), 2010 IEEE Second International Conference on*, pages 1165–1170, 2010c. DOI 10.1109/SocialCom.2010.173.

COSO. Enterprise risk management - integrated framework - executive summary. Technical report, Commitee of the Sponsoring Organizations of the Treadway Organization, 2004. URL http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf. (Visited on 2013-05-17).

COSO. Commitee of the sponsoring organizations of the treadway commission (draft). Technical report, Commitee of the Sponsoring Organizations of the Treadway Commission, 2011.

COSO. Internal control - integrated framework - executive summary. Technical report, Commitee of the Sponsoring Organizations of the Treadway Organization, 2013. URL http://www.coso.org/documents/COSO%202013%20ICFR%20Executive_Summary.pdf. (Visited on 2013-05-17).

William Edwards Deming. *Out of the Crisis*. The MIT Press, 2000. URL http://books.google.at/books?id=LA15eDlOPgoC. (Visited on 2012-12-09).

European-Parliament. Directive 2006/43/ec. *Official Journal of the European Union*, 2006. URL http://www.esma.europa.eu/system/files/dir_2006_43_EN.pdf. (Visited on 2013-06-10).

FERMA. A risk management standard. Technical report, Federation of European Risk Management Associations, 2002. URL http://www.ferma.eu/wp-content/uploads/2011/11/a-risk-management-standard-english-version.pdf. (Visited on 2013-05-17).

Heinz von Foerster. Cybernetics of cybernetics. In *Understanding Understanding – Essays on Cybernetics and Cognition*, pages 283–286. Springer, 2003. URL http://books.google.at/books?id=mAkIVn9d-9kC. (Visited on 2012-12-09).

G31000. Global iso 31000 survey 2011 - results and analysis. Technical report, ISO 31000 Conference by the G31000 the Global Risk Management Platform, 2012. URL http://www.iso31000survey.com/Global_Survey_ISO_31000_English.pdf. (Visited on 2013-05-18).

Carl A. Gibson and Michael Tarrant. A 'conceptual models' approach to organisational resilience. *The Australian Journal of Emergency Management*, 25(2):6–12, April 2010. URL http://www.em.gov.au/Documents/A%20%20conceptual%20models%20%20approach%20to%20organisational%20resilience.PDF. (Visited on 2013-04-17).

Dorothy Gjerdrum and Mary Peter. The new international standard on the practice of risk management - a comparison of iso 31000:2009 and the coso erm framework. *Risk Management*, 21:8–13, 2011. URL http://www.soa.org/library/newsletters/risk-management-newsletter/2011/march/jrm-2011-iss21.pdf. (Visited on 2013-05-19).

Lace Gunderson, Ahjond S. Garmestani, and Craig R. Allen. Panarchy: Discontinuities reveal similarities in the dynamic system structure of ecological and social systems. *Ecology and Society*, 14, 2009. URL http://www.ecologyandsociety.org/vol14/iss1/art15/. (Visited on 2013-06-05).

Gary Hamel and Liisa Valikangas. The quest for resilience. *Harvard Business Review*, 81: 52–65, 2003. URL http://hbr.org/2003/09/the-quest-for-resilience. (Visited on 2013-06-10).

Alan R. Hevner. Design science in information systems research. *MIS Quaterly*, 28:75–105, 2004. URL http://dl.acm.org/citation.cfm?id=2017212.2017217. (Visited on 2013-07-17).

IRM. Risk culture. Technical report, Institute of Risk Management, 2012. URL http://www.theirm.org/documents/Risk_Culture_A5_WEB15_Oct_2012.pdf. (Visited on 2013-05-17).

ISO. Iso-31000 risk management - principles and guidelines. Technical report, International Organization for Standardization, 2009. URL http://www.iso.org/iso/home/standards/iso31000.htm. (Visited on 2012-12-10).

Frederic Jameson. *Postmodernism, or The cultural Logic of Late Capitalism*. Duke University Press Durham, 1991. URL http://books.google.at/books?id=oRJ9fh9BK8wC. (Visited on 2013-05-17).

Daniel Kahnemann. *Schnelles Denken, langsames Denken*. Siedler Verlag, 2012. URL http://books.google.at/books?id=4tV9qDT0CpoC. German. (Visted on 2013-05-17).

Robert S. Kaplan and Anette Mikes. Managing risks: A new framework. *Harvard Busienss Review*, 90:48–60, 6 2012. URL http://hbr.org/2012/06/managing-risks-a-new-framework/ar/. (Visited on 2013-05-17).

Robert S. Kaplan and Anette Mikes. Managing risks: towards a contingency theory of enterprise risk management. Technical report, Harvard Business School, 2013. URL http://www.hbs.edu/faculty/Publication%20Files/13-063_b87e3389-4c24-4662-8906-47085ea749bf.pdf. (Visited on 2013-05-17).

Sonia T. McManus. *Organisational Resiliense in New Zealand*. PhD thesis, University of Canterbury, 2008. URL http://ir.canterbury.ac.nz/bitstream/10092/1574/1/thesis_fulltext.pdf. (Visited on 2012-11-04).

Anette Mikes. From counting risk to making risk count: Boundrary-work in risk management. Technical report, Harvard Business School, 2011. URL http://www.hbs.edu/faculty/Publication%20Files/11-069.pdf. (Visited on 2013-06-09).

Arnette Mikes. Risk management and calculative cultures. *Management Accounting Research*, 20:pp. 18–40, 2009. DOI 10.1016/j.mar.2008.10.005.

OMG. Unified modelling language. Technical report, Object Management Group, 2011. URL http://www.omg.org/spec/UML/2.4.1/Infrastructure/PDF. (Visited on 2012-12-09).

Charles A. O'Reilly and Michael T. L. Tushman. The ambidextrous organiztion. *Harvard Business Review*, 82:74–83, 2004. URL http://hbr.org/2004/04/the-ambidextrous-organization/. (Visited on 2013-06-12).

Kevin G. Partridge and Lisa R. Young. Cert resilience management model (rmm) v1.1: Code of practice crowsswalk commercial version 1.1). Technical report, Software Engineering Institute (SEI), 2011. URL http://www.sei.cmu.edu/reports/11tn012.pdf. (Visited on 2013-04-08).

Michael E. Porter. *Competitive advantage: Creating and sustaining superior performance*. Free press, 2008. URL http://books.google.at/books?id=H9ReAijCK8cC. (Visited on 2013-05-18).

Michael Power. The risk management of nothing. *Accounting, Organizations and Society*, 34: 849–855, 2009. DOI 10.1016/j.aos.2009.06.001.

PWC. Managing risk: An assessment of ceo preparedness. Technical report, PriceWaterhouseCoopers, 2004. URL http://www.pwc.fr/fr/pwc_pdf/pwc_ceo_2004.pdf. (Visited on 2013-05-19).

PWC. Extending enterprise risk management (erm) to addressing emergent risks. Technical report, PriceWaterhouseCoopers, 2009. URL http://www.pwc.com/gx/en/research-publications/pdf/pwcglobalriskserm.pdf. (Visited on 2013-05-19).

RIMS. Rims executive report - the risk perspective. Technical report, Risk and Insurance Management Society (RIMS), 2011. URL http://www.rims.org/resources/ERM/Documents/RIMS%20Executive%20Report%20on%20Widely%20Used%20Standards%20and%20Guidelines%20March%202010.pdf. (Visited on 2013-06-02).

Walter S. A. Schwaiger. Risk management: Comprehensive integration into the enterprise management. In *Asset Management - Festschrift für Prof. Dr. rer. nat. Dr. h.c. rer. pol. Klaus Spremann zur Emeritierung*, chapter 4, pages 420–459. Haupt Verlag, 2012. URL http://www.haupt.ch/verlag/FACHBUCH/Wirtschaft-Recht/Gesamtverzeichnis/Bank-Finanz/Asset-Management.html. (Visited on 2012-11-12).

Markus Schwaninger. Managing complexity - the path toward intelligent organizations. *System Practice and Action Research*, 12:207–241, 2000. DOI 10.1023/A:1009546721353.

Markus Schwaninger. System theory and cybernetics. a solid basis for transdisciplinarity in management education and research. *Systems theory and cybernetics*, 30:1209–1222, 2001a. DOI 10.1108/EUM0000000006551.

Markus Schwaninger. Intelligent organizations: An integrative framework. *Systems Research and Behavioral Science*, 18:137–158, 2001b. DOI 10.1002/sres.408.

Denis Smith and Moira Fischbacher. The changing nature of risk and risk management: The challenge of borders, uncertainty and resilience. *Risk Management*, 11:1–12, 2009. DOI 10.1057/rm.2009.1.

Amy Stephenson. *Benchmarking the Resilience of Organisations*. PhD thesis, University of Canterbury, 2010. URL http://ir.canterbury.ac.nz/bitstream/10092/5303/1/THESIS_BENCHMARKINGTHERESILIENCEOFORGANISATIONS.pdf. (Visited on 2012-11-04).

Kathleen M. Sutcliffe and Timothy J. Vogus. Organizing for resilience. In Kim S. Cameron, Jane E. Dutton, and Quinn Robert E., editors, *Positive Organizational Scholarship*, chapter 7, pages 94–110. Berret Koehler Publishers Inc., 2003. URL http://owen.vanderbilt.edu/vanderbilt/data/research/1587full.pdf. (Visited on 2012-10-30).

Kathleen M. Sutcliffe and Timothy J. Vogus. Organizational resilience: Towards a theory and research agenda. In *Conference on Systems, Man and Cybernetics*, pages 3418–3422. IEEE International, 2007. DOI 10.1109/ICSMC.2007.4414160.

Nassim Nicholas Taleb. *Antifragilität*. Albrecht Knaus Verlag, 2013. URL http://books.google.at/books?id=K8BFbR25ggwC. German. (Visited on 2013-05-17).

US-Congress. Sarbanes-oxley act of 2002. corporate responsibility. *Public Law 107-204*, 2002. URL http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf. (Visited on 2013-06-10).

Joan Ernst van Aken and Georges Romm. Reinventing the future: adding design science to the repertoire of organization and management studies. *Organization Management Journal*, 6: 5–12, 2009. DOI 10.1057/omj.2009.1.

WEF. *Global Risks 2012*. Word Economic Forum, 2012. URL http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf. (Visited on 2013-05-15).

WEF. *Global Risks 2013*. Word Economic Forum, 2013. URL http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf. (Visited on 2013-05-15).

Karl E. Weick. The collapse of sensemaking in organizations: The mann gulch disaster. *Administrative Science Quarterly*, 38(4):628–652, 1993. DOI 10.2307/2393339.

Karl E. Weick. *Sensemaking in organizations*, volume 3. Sage Publications, Incorporated, 1995. URL http://books.google.at/books?id=nz1RT-xskeoC. (Visited on 2012-10-30).

Karl E. Weick. *Making Sense of the Organization*, volume 1 of *KeyWorks in Cultural Studies*. Blackwell Publishers, 2001. ISBN 9780631223191. URL http://books.google.at/books?id=agZzW4mqS4wC. (Visited on 2012-10-30).

Karl E. Weick and Kathleen M. Sutcliffe. *Das unerwartete Managen: Wie Unternehmen aus Extremsituationen lernen*. Klett-Cotta, 2003. URL http://books.google.at/books?id=gcuRAAAACAAJ. (Visited on 2012-10-30).

Karl E. Weick, Kathleen M. Sutcliffe, and David Obstfeld. Organizing for high reliability: Prozesses of collective mindfulness. In Arjen Boin, editor, *Crisis Management*, volume 3, pages 31–66. SAGE, 2008. URL http://www2.comm.niu.edu/faculty/rholt/eocg/LLRreadUnit3BWeickEtAl.pdf. (Visited on 2012-10-30).

Karl El Weick. *Making Sense of the Organization - The Impermanent Organization*, volume 2. John Wiley & Sons Ltd, 2009. URL http://books.google.at/books?id=2IMF4iwKeHoC. (Visited on 2012-31-10).

Norbert Wiener. *Kybernetik - Regelung und Nachrichtenübertragung im Lebewesen und in der Maschine*. Econ Verlag, 1963. URL http://books.google.at/books?id=sCQtpwAACAAJ. (Visited on 2012-12-09).

APPENDIX A

Tables Appendix

A.1 Stephenson's Indicators of Organizational Resilience

Resilience Attribute	Resilience Indicator	Indicator Description
Adaptive Capacity	Minimisation of Silo Mentality	Minimisation of divisive social, cultural and behavioural barriers, which are most often manifested as communication barriers creating disjointed, disconnected and detrimental ways of working.
	Capability & Capacity of Internal Resources	The management and mobilisation of the organisation's resources to ensure its ability to operate during business as usual , as well as being able to provide the extra capacity required during a crisis.
	Staff Engagement & Involvement	The engagement and involvement of staff who understand the link between their own work, the organisation's resilience, and its long term success. Staff are empowered and use their skills to solve problems.
	Information & Knowledge	Critical information is stored in a number of formats and locations and staff have access to expert opinions when needed. Roles are shared and staff are trained so that someone will always be able to fill key roles.
	Leadership, Management & Governance Structures	Strong crisis leadership to provide good management and decision making during times of crisis, as well as continuous evaluation of strategies and work programs against organizational goals.
	Innovation & Creativity	Staff are encouraged and rewarded for using their knowledge in novel ways to solve new and existing problems, and for utilizing innovative and creative approaches to developing solutions.

Resilience Attribute	Resilience Indicator	Indicator Description
	Devolved & Responsive Decision Making	Staff have the appropriate authority to make decisions related to their work and authority is clearly delegated to enable a crisis response. Highly skilled staff are involved, or are able to make, decisions where their specific knowledge adds significant value, or where their involvement will aid implementation.
	Internal & External Situation Monitoring & Reporting	Staff are encouraged to be vigilant about the organisation, its performance and potential problems. Staff are rewarded for sharing good and bad news about the organisation including early warning signals and these are quickly reported to organizational leaders.
Planning	Planning Strategies	The development and evaluation of plans and strategies to manage vulnerabilities in relation to the business environment and its stakeholders.
	Participation in Exercises	The participation of staff in simulations or scenarios designed to practice response arrangements and validate plans.
	Proactive Posture	A strategic and behavioural readiness to respond to early warning signals of change in the organisation's internal and external environment before they escalate into crisis.
	Capability & Capacity of External Resources	An understanding of the relationships and resources the organisation might need to access from other organisations during a crisis, and planning and management to ensure this access.
	Recovery Priorities	An organisation wide awareness of what the organisation's priorities would be following a crisis, clearly defined at the organisation level, as well as an understanding of the organisation's minimum operating requirements.

Table A.1: Stephenson's Indicators of Organizational Resilience

A.2 Comparison of ASIS Resilience Management Activities with CERT Resilience Metrics

CERT-RMM Specific Goal/Practice	ASIS Resilience Activities	CERT Metrics
COMM:SG1 Prepare for Resilience Communications		
COMM:SG1.SP1 Identify Relevant Stakeholders	4.4.3 Communication and Warning	COMM-M1, COMM-M2, COMM-M3
COMM:SG1.SP2 Identify Communications Requirements	-	COMM-M4
COMM:SG1.SP3 Establish Communications Guidelines and Standards	-	COMM-M19
COMM:SG2 Prepare for Communications Management		
COMM:SG2.SP1 Establish a Resilience Communications Plan	4.3.2 Legal and Other Requirements 4.4.2 Competence, Training, and Awareness	COMM-M20
COMM:SG2.SP2 Establish a Resilience Communications Program	4.4.2 Competence, Training, and Awareness	COMM-M5, COMM-M6
COMM:SG2.SP3 Identify and Assign Plan Staff	4.4.1 Resources, Roles, Responsibility, and Authority A.4.3 Communication and Warning	COMM-M5, COMM-M6
COMM:SG3 Deliver Resilience Communications		
COMM:SG3.SP1 Identify Communications Methods and Channels	-	COMM-M7, COMM-M9
COMM:SG3.SP2 Establish and Maintain Communications Infrastructure	4.4.3.j Communications and Warning	COM-M5
COMM:SG4 Improve Communications		
COMM:SG4.SP1 Assess Communications Effectiveness	A.4.3 Communication and Warning	COMM-M10, COMM-M11, COMM-M12, COMM-M13, COMM-M14, COMM-M15, COMM-M16
COMM:SG4.SP2 Improve Communications	-	COMM-M17, COMM-M18
COMP:SG1 Prepare for Compliance Management		
COMP:SG1.SP1 Establish a Compliance Plan	4.3.2 Legal and Other Requirements	COMP-M1, COMP-M13

CERT-RMM Specific Goal/Practice	ASIS Resilience Activities	CERT-RMM Metrics
COMP:SG1.SP2 Establish a Compliance Program	4.3.2 Legal and Other Requirements	COMP-M2, COMP-M13, COMP-M14, COMP-M15
COMP:SG1.SP3 Establish Compliance Guidelines and Standards	4.3.2 Legal and Other Requirements	COMP-M2, COMP-M6
COMP:SG2 Establish Compliance Obligations		
COMP:SG2.SP1 Identify Compliance Obligations	-	COMP-M3, COMP-M4, COMP-M5, COMP-M6, COMP-M7, COMP-M8, COMP-M19
COMP:SG2.SP2 Analyze Obligations	-	COMP-M16
COMP:SG2.SP3 Establish Ownership for Meeting Obligations	-	COMP-M5
COMP:SG3 Demonstrate Satisfaction of Compliance Obligations		
COMP:SG3.SP1 Collect and Validate Compliance Data	-	COMP-M22
COMP:SG3.SP2 Demonstrate the Extent of Compliance Obligation Satisfaction	-	COMP-M9, COMP-M10, COMP-M11, COMP-M14, COMP-M19
COMP:SG3.SP3 Remediate Areas of Non-Compliance	-	COMP-M14, COMP-M17
COMP:SG4 Monitor Compliance Activities		
COMP:SG4.SP1 Evaluate Compliance Activities	4.5.2.1 Evaluation of Compliance	COMP-M12, COMP-M18, COMP-M20, COMP-M21
EF:SG1 Establish Strategic Objectives		
EF:SG1.SP1 Establish Strategic Objectives	4.4.1.a Goals & Mission of the Organization (Scope)	-
EF:SG1.SP2 Establish Critical Success Factors	4.4.1.c Critical Operational Objectives, Assets, Functions, Services, and Products (Scope)	EF-M1
EF:SG1.SP3 Establish Organizational Services	4.4.1.c Critical Operational Objectives, Assets, Functions, Services, and Products (Scope)	EF-M2, EF-M3, EF-M4

CERT-RMM Specific Goal/Practice	ASIS Resilience Activities	CERT-RMM Metrics
EF:SG2 Plan for Operational Resilience		
EF:SG2.SP1 Establish an Operational Resilience Management Plan	4.4.4 Documentation incl. Objectives, Do-, Measure-, & Act-Rules)	EF-M5, EF-M6
EF:SG2.SP2 Establish an Operational Resilience Management Program	4.1.1 Scope of the OR Management System 4.4.4 Documentation	EF-M7
EF:SG3 Establish Sponsorship		
EF:SG3.SP1 Commit Funding for Operational Resilience Management	4.4.1 Resources, Roles, Responsibility, and Authority	EF-M7, EF-M8, EF-M27
EF:SG3.SP2 Promote a Resilience-Aware Culture	4.4.2 Competence, Training, and Awareness	EF-M9, EF-M10, EF-M11, EF-M12, EF-M13, EF-M14
EF:SG3.SP3 Sponsor Resilience Standards and Policies	4.2.1 Policy Statement	EF-M15
EF:SG4 Provide Resilience Oversight		
EF:SG4.SP1 Establish Resilience as a Governance Focus Area	4.5.5 Internal Audits	EF-M15, EF-M16, EF-M17, EF-M18
EF:SG4.SP2 Perform Resilience Oversight	4.5.2.1 Evaluate Compliance 4.5.2.2 Exercises, Testing, Evaluate Performance	EF-M10, EF-M11, EF-M19, EF-M20, EF-M22, EF-M23, EF-M24, EF-M25, EF-M26, EF-M27, EF-M28, EF-M29, EF-M29, EF-M20, EF-M31, EF-M32, EF-M33
EF:SG4.SP3 Establish Corrective Actions	4.5.3 Nonconformity, Corrective-, and Preventive Action	EF-M20, EF-M21
OTA:SG1 Establish Awareness Program		

CERT-RMM Specific Goal/Practice	ASIS Resilience Activities	CERT-RMM Metrics
OTA:SG1.SP1 Establish Awareness Need	4.4.2 Competence, Training, and Awareness	OTA-M1,
OTA:SG1.SP2 Establish Awareness Training Plan	A.4.2 Competence, Training, and Awareness	OTA-M1, OTA-M2, OTA-M3
OTA:SG1.SP3 Establish Awareness Training Capability	-	OTA-M4
OTA:SG2 Conduct Awareness Activities		
OTA:SG2.SP1 Perform Awareness Activities	4.5.2.2 Exercises, Testing, Evaluate Performance	OTA-M2, OTA-M3
OTA:SG2.SP2 Establish Awareness Records	-	OTA-M5, OTA-M6, OTA-M10
OTA:SG2.SP3 Assess Awareness Program Effectiveness	-	OTA-M7, OTA-M8, OTA-M9
OTA:SG3 Establish Training Capability		
OTA:SG3.SP1 Establish Training Needs	-	OTA-M11
OTA:SG3.SP2 Establish Training Plan	-	OTA-M11, OTA-M12, OTA-M13
OTA:SG3.SP3 Establish Training Capability	-	OTA-M15
OTA:SG4 Conduct Training		
OTA:SG4.SP1 Deliver Training	-	OTA-M12, OTA-M16, OTA-M17
OTA:SG4.SP2 Establish Training Records	-	OTA-M19, OTA-M21
OTA:SG4.SP3 Assess Training Effectiveness	4.5.2.2 Exercises, Testing, Evaluate Performance	OTA-M14, OTA-M18, OTA-M20
RISK:SG1 Prepare for Risk Management		
RISK:SG1.SP1 Determine Risk Sources and Categories	4.3.1 Risk Assessment and Impact Analysis	RISK-M1, RISK-M2, RISK-M3, RISK-M4, RISK-M5
RISK:SG1.SP2 Establish an Operational Risk Management Strategy	4.3.1 Risk Assessment and Impact Analysis	RISK-M6, RISK-M7

CERT-RMM Specific Goal/Practice	ASIS Resilience Activities	CERT-RMM Metrics
RISK:SG2 Establish Risk Parameters and Focus		
RISK:SG2.SP1 Define Risk Parameters	4.3.1 Risk Assessment and Impact Analysis	RISK-M8, RISK-M9
RISK:SG2.SP2 Establish Risk Measurement Criteria	4.3.1 Risk Assessment and Impact Analysis	RISK-M10, RISK-M11
RISK:SG3 Identify Risk		
RISK:SG3.SP1 Identify Asset-Level Risks	4.1.1 Scope of OR Management System 4.2.1 Policy Statement	RISK-M12, RISK-M13, RISK-M14, RISK-M16, RISK-M17
RISK:SG3.SP2 Identify Service-Level Risks	4.1.1 Scope of OR Management System 4.2.1 Policy Statement	RISK-M15, RISK-M16, RISK-M17
RISK:SG4 Analyze Risk		
RISK:SG4.SP1 Evaluate Risk	4.3.1 Risk Assessment and Impact Analysis	RISK-M18, RISK-M20, RISK-M21
RISK:SG4.SP2 Categorize and Prioritize Risk	4.3.1 Risk Assessment and Impact Analysis	RISK-M17, RISK-M19, RISK-M21
RISK:SG4.SP3 Assign Risk Disposition	4.4.7 Prevention, Preparedness, and Response 4.4.2 Competence, Training, and Awareness	RISK-M22, RISK-M24
RISK:SG5 Mitigate and Control Risk		
RISK:SG5.SP1 Develop Risk Mitigation Plans	4.4.7 Prevention, Preparedness, and Response	RISK-M23, RISK-M25, RISK-M26, RISK-M27
RISK:SG5.SP2 Implement Risk Strategies	4.4.7 Prevention, Preparedness, and Response	RISK-M26, RISK-M27, RISK-M28, RISK-M29, RISK-M30, RISK-M31, RISK-M32, RISK-M34
RISK:SG6 Use Risk Information to Manage Resilience		
RISK:SG6.SP1 Review and Adjust Strategies to Protect Assets and Services	4.4.7 Prevention, Preparedness, and Response	RISK-M28, RISK-M29
RISK:SG6.SP2 Review and Adjust Strategies to Sustain Services	-	RISK-M28, RISK-M29

CERT-RMM Specific Goal/Practice	ASIS Resilience Activities	CERT-RMM Metrics
ADM:SG1 Establish Organizational Assets		
ADM:SG1.SP1 Inventory Assets	4.1.1 Scope of the OR Management System 4.3.1 Risk Assessment and Impact Analysis	ADM-1, ADM-M9
ADM:SG1.SP2 Establish a Common Understanding	4.3.1 Risk Assessment and Impact Analysis	ADM-M2
ADM:SG1.SP3 Establish Ownership and Custodianship	-	ADM-M3, ADM-M4, ADM-M5, ADM-M6
ADM:SG2 Establish Relationship Between Assets and Services		
ADM:SG2.SP1 Associate Assets with Services	4.3.1 Risk Assessment and Impact Analysis	ADM-M7, ADM-M8
ADM:SG2.SP2 Analyze Asset-Service Dependencies	4.3.1 Risk Assessment and Impact Analysis	ADM-M11
ADM:SG3 Manage Assets		
ADM:SG3.SP1 Identify Change Criteria	-	ADM-M9, ADM-M12
ADM:SG3.SP2 Maintain Changes to Assets and Inventory	-	ADM-M10, ADM-M13, ADM-M14, ADM-M15
SC:SG1 Prepare for Service Continuity		
SC:SG1.SP1 Plan for Service Continuity	4.3.3 Objectives, Targets, and Programs 4.4.7 Incident Prevention, Preparedness, and Response	SC-M1, SC-M2, SC-M3
SC:SG1.SP2 Establish Standards and Guidelines for Service Continuity	4.4.3 Communication and Warning 4.5.4 Control of Records	SC-M1, SC-M3
SC:SG2 Identify and Prioritize High-Value Services		
SC:SG2.SP1 Identify the Organization's High-Value Services	4.1.1 Scope of the OR Management System 4.3.1 Risk Assessment and Impact Analysis	SC-M8
SC:SG2.SP2 Identify Internal and External Dependencies and Interdependencies	4.3.1 Risk Assessment and Impact Analysis	SC-M4, SC-M5
SC:SG2.SP3 Identify Vital Organizational Records and Databases	-	SC-M6
SC:SG3 Develop Service Continuity Plans		

CERT-RMM Specific Goal/Practice	ASIS Resilience Activities	CERT-RMM Metrics
SC:SG3.SP1 Identify Plans to be Developed	-	SC-M8
SC:SG3.SP2 Develop and Document Service Continuity Plans	4.4.4 Documentation 4.4.6. Operational Control 4.4.7 Incident Prevention, Preparedness, and Response	SC-M7, SC-M11, SC-M12, SC-M13
SC:SG3.SP3 Assign Staff to Service Continuity Plans	4.4.5 Control of Documents 4.5.4 Control of Records 4.4.7 Incident Prevention, Preparedness, and Response	SC-M14, SC-M15
SC:SG3.SP4 Store and Secure Service Continuity Plans	4.4.5 Control of Documents 4.5.4 Control of Records	SC-M9, SC-M27, SC-M28
SC:SG3.SP5 Develop Service Continuity Plan Training	-	SC-M19
SC:SG4 Validate Service Continuity Plans		
SC:SG4.SP1 Validate Plans to Requirements and Standards	-	SC-M16, SC-M17
SC:SG4.SP2 Identify and Resolve Plan Conflicts	-	SC-M10, SC-M20
SC:SG5 Exercise Service Continuity Plans	-	
SC:SG5.SP1 Develop Testing Program and Standards	4.5.2.2 Exercise and Training 4.4.7 Incident Prevention, Preparedness, and Response	SC-M21
SC:SG5.SP2 Develop and Document Test Plans	4.5.3 Nonconformity, Corrective Action, and Preventive Action	SC-M22
SC:SG5.SP3 Exercise Plans	-	SC-M23, SC-M24, SC-M28
SC:SG5.SP4 Evaluate Plan Test Results	-	SC-M25, SC-M26
SC:SG6 Execute Service Continuity Plans		
SC:SG6.SP1 Execute Plans	-	SC-M30
SC:SG6.SP2 Measure the Effectiveness of the Plan in Operation	4.5.3 Nonconformity, Corrective Action, and Preventive Action	SC-M31
SC:SG7 Maintain Service Continuity Plans		
SC:SG7.SP1 Establish Change Criteria	-	SC-M32
SC:SG7.SP2 Maintain Changes to Plans	4.4.5 Control of Documents	SC-M32, SC-M22, SC-M34, SC-M35, SC-M36

CERT-RMM Specific Goal/Practice	ASIS Resilience Activities	CERT-RMM Metrics
IMC:SG1 Establish the Incident Management and Control Process		
IMC:SG1.SP1 Plan for Incident Management	4.4.7 Incident, Prevention, Preparedness, and Response	IMC-M1
IMC:SG1.SP2 Assign Staff to the Incident Management Plan	4.4.7 Incident, Prevention, Preparedness, and Response	IMC-M2, IMC-3
IMC:SG2 Detect Events		
IMC:SG2.SP1 Detect and Report Events	4.4.7 Incident, Prevention, Preparedness, and Response	IMC-M2, IMC-M4, IMC-M6
IMC:SG2.SP2 Log and Track Events	4.4.7 Incident, Prevention, Preparedness, and Response	IMC-M6, IMC-M11
IMC:SG2.SP3 Collect, Document, and Preserve Event Evidence	-	IMC-M7
IMC:SG2.SP4 Analyze and Triage Events	4.4.7 Incident, Prevention, Preparedness, and Response	IMC-M5, IMC-M8, IMC-M9, IMC-M10
IMC:SG3 Declare Incidents		
IMC:SG3.SP1 Define and Maintain Incident Declaration Criteria	4.4.7 Incident, Prevention, Preparedness, and Response	IMC-M14
IMC:SG3.SP2 Analyze Incidents	4.4.7 Incident, Prevention, Preparedness, and Response	IMC-M12, IMC-M13, IMC-M14, IMC-M17, IMC-M23
IMC:SG4 Respond to and Recover from Incidents		
IMC:SG4.SP1 Escalate Incidents	4.4.7 Incident, Prevention, Preparedness, and Response	IMC-M15, IMC-M16, IMC-M30
IMC:SG4.SP2 Develop Incident Response	4.4.7 Incident, Prevention, Preparedness, and Response	-
IMC:SG4.SP3 Communicate Incidents	4.4.7 Incident, Prevention, Preparedness, and Response	IMC-M31, IMC-M32
IMC:SG4.SP4 Close Incidents	4.4.7 Incident, Prevention, Preparedness, and Response	IMC-M12, IMC-M16
IMC:SG5 Establish Incident Learning		

CERT-RMM Specific Goal/Practice	ASIS Resilience Activities	CERT-RMM Metrics
IMC:SG5.SP1 Perform Post-Incident Review	4.5 Checking	IMC-M13, IMC-M17, IMC-M18, IMC-M19, IMC-M20, IMC-M21, IMC-M22, IMC-M23, IMC-M24, IMC-M25, IMC-M26, IMC-M27, IMC-M28, IMC-M33
IMC:SG5.SP2 Integrate with the Problem Management Process	-	IMC-M34
VAR:SG1 Prepare for Vulnerability Analysis and Resolution		
VAR:SG1.SP1 Establish Scope	4.1.1 ORM Scope	-
VAR:SG1.SP2 Establish a Vulnerability Analysis and Resolution Strategy	4.3.1 Risk Assessment and Impact Analysis	-
VAR:SG2 Identify and Analyze Vulnerabilities		
VAR:SG2.SP1 Identify Sources of Vulnerability Information	4.4.3 Communication and Warning	-
VAR:SG2.SP2 Discover Vulnerabilities	4.3.1 Risk Assessment and Impact Analysis	VAR-M3
VAR:SG2.SP3 Analyze Vulnerabilities	4.3.1 Risk Assessment and Impact Analysis	VAR-M4, VAR-M14
VAR:SG3 Manage Exposure to Vulnerabilities		
VAR:SG3.SP1 Manage Exposure to Vulnerabilities	4.4.7 Incident, Prevention, Preparedness, and Response	VAR-M5, VAR-M6, VAR-M7, VAR-M8
VAR:SG4 Identify Root Causes		
VAR:SG4.SP1 Perform Root-Cause Analysis	-	VAR-M9, VAR-M10
MA:SG1 Align Measurement and Analysis Activities		
MA:SG1.SP1 Establish Measurement Objectives	4.3.3 Objectives and Targets	MA-M1, MA-M7
MA:SG1.SP2 Specify Measures	4.3.1 Risk and Hazard Measures	MA-M2

CERT-RMM Specific Goal/Practice	ASIS Resilience Activities	CERT-RMM Metrics
MA:SG1.SP3 Specify Data Collection and Storage Procedures	-	MA-M9
MA:SG1.SP4 Specify Analysis Procedures	-	MA-M9
MA:SG2 Provide Measurement Results		
MA:SG2.SP1 Collect Measurement Data	4.2.2.g Level of Risks A.3.1.i Level of Resilience	MA-M4, MA-M6, MA-M7, MA-M8, MA-M9
MA:SG2.SP2 Analyze Measurement Data	-	MA-M3, MA-M4, MA-M6, MA-M8, MA-M9
MA:SG2.SP3 Store Data and Results	-	MA-M8, MA-M9
MA:SG2.SP4 Communicate Results	-	MA-M4, MA-M5, MA-M6
MON:SG1 Establish and Maintain a Monitoring Program		
MON:SG1.SP1 Establish Monitoring Program	4.5.1 Monitoring and Measurement	
MON:SG1.SP2 Identify Stakeholders	-	MON-M8
MON:SG1.SP3 Establish Monitoring Requirements	-	MON-M3, MON-M4, MON-M7
MON:SG1.SP4 Analyze and Prioritize Monitoring Requirements	-	MON-M3, MON-M4, MON-M5
MON:SG2 Perform Monitoring		
MON:SG2.SP1 Establish and Maintain Monitoring Infrastructure	-	
MON:SG2.SP2 Establish Collection Standards and Guidelines	-	
MON:SG2.SP3 Collect and Record Information	-	MON-M1, MON-M9
MON:SG2.SP4 Distribute Information	-	MON-M1, MON-M6

Table A.2: Matching of CERT-RMM Specific Practices, Metrics and ASIS Resilience Management Activities

A.3 Comparison of ISO 31000 Risk Management Activities with CERT Resilience Metrics

CERT-RMM Specific Goal/Practice	ISO 31000 Risk Management Activities	CERT Metrics
RISK:SG1 Prepare for Risk Management		
RISK:SG1.SP1 Determine Risk Sources and Categories	-	RISK-M1, RISK-M2, RISK-M3, RISK-M4, RISK-M5
RISK:SG1.SP2 Establish an Operational Risk Management Strategy	5.1 General RM Process 5.2 Communication and Consultation 5.3.1 Establishing the Context 5.3.2 Establishing the External Context 5.3.3 Establishing the Internal Context 5.3.4 Establishing the Context of the RM Process	RISK-M6, RISK-M7
RISK:SG2 Establish Risk Parameters and Focus		
RISK:SG2.SP1 Define Risk Parameters	5.3.5 Defining Risk Criteria	RISK-M8, RISK-M9
RISK:SG2.SP2 Establish Risk Measurement Criteria	5.3.5 Defining Risk Criteria	RISK-M10, RISK-M11
RISK:SG3 Identify Risk		
RISK:SG3.SP1 Identify Asset-Level Risks	5.4.2 Risk Identification	RISK-M12, RISK-M13, RISK-M14, RISK-M16, RISK-M17
RISK:SG3.SP2 Identify Service-Level Risks	5.4.2 Risk Identification	RISK-M15, RISK-M16, RISK-M17
RISK:SG4 Analyze Risk		
RISK:SG4.SP1 Evaluate Risk	5.4.3 Risk Analysis	RISK-M18, RISK-M20, RISK-M21
RISK:SG4.SP2 Categorize and Prioritize Risk	5.4.4 Risk Evaluation	RISK-M17, RISK-M19, RISK-M21
RISK:SG4.SP3 Assign Risk Disposition	5.4.4 Risk Evaluation	RISK-M22, RISK-M24
RISK:SG5 Mitigate and Control Risk		
RISK:SG5.SP1 Develop Risk Mitigation Plans	5.5.1 General Risk Treatment 5.5.2 Selection of Risk Treatment Options	RISK-M23, RISK-M25, RISK-M26, RISK-M27

CERT-RMM Specific Goal/Practice	**ISO 31000 Risk Management Activities**	**CERT-RMM Metrics**
RISK:SG5.SP2 Implement Risk Strategies	5.5.3 Preparing and Implementing Risk Treatment Plans	RISK-M26, RISK-M27, RISK-M28, RISK-M29, RISK-M30, RISK-M31, RISK-M32, RISK-M34
RISK:SG6 Use Risk Information to Manage Resilience		
RISK:SG6.SP1 Review and Adjust Strategies to Protect Assets and Services	5.6 Monitoring and Review 5.7 Recording the Risk Management Process	RISK-M28, RISK-M29
RISK:SG6.SP2 Review and Adjust Strategies to Sustain Services	5.6 Monitoring and Review 5.7 Recording the Risk Management Process	RISK-M28, RISK-M29

Table A.3: Matching of CERT-RMM Specific Practices, Metrics and ISO 31000 Risk Management Activities