

# Improving information security compliance – A process-oriented approach for managing organizational change

Prof. Dr. Roland Gabriel, Sebastian Sowa, Jochen Wiedemann

Institute for E-Business Security (ISEB),  
Ruhr-University of Bochum, GC 3/29, 44780 Bochum, Germany  
rgabriel@winf.ruhr-uni-bochum.de  
sebastian.sowa@ruhr-uni-bochum.de  
jochen.wiedemann@ruhr-uni-bochum.de

**Abstract:** Enterprises typically have to comply with many different legal, regulatory and internal requirements. Particularly in the context of information processing, there are dedicated regulations which demand the protection of the information infrastructure. From the authors' point of view, organizational aspects are thereby one of the most critical improvement areas. However, the related organizational change process can be challenging in order to appropriately define and anchor adequate roles within the organization. To align the organization to the specific requirements of information security (IS), it is necessary to change the current organizational state into one that better supports the IS compliance performance. A process-oriented approach for managing the organizational change to improve information security compliance is presented in this contribution. The approach uses Business Aligned Information Security Management (BAISem) and principles that have been derived from standards like ITIL, COBIT and ISO 27001. In order to illustrate the approach, the context of IT service continuity is selected as an example.

## 1 Introduction

In the year 2006, CA conducted a survey to identify current trends in information security (IS), with 224 online questionnaires regarding experiences, challenges and objectives of each enterprise in the IS context analyzed and evaluated. One of the key findings: More than 50% of the enterprises declared an increase of compliance importance but only 20% already had an IS certification although these certificates are an integral aspect of compliance requirements confirmation [CA06].

When talking about compliance, different legal, regulatory and internal requirements can be relevant for the enterprise [Mü05]. In the compliance context, this paper focuses on standards concentrating furthermore on ITIL, COBIT and ISO 27001. To prepare for a security certification, the enterprise typically has to implement additional measures and set up an appropriate management process [Ec05]. This management process often is included within information risk management to identify, assess and manage relevant operational risks. However, in this context many enterprises focus on low-level security management activities without considering the compliance and organizational aspects.

Thereby, managing the organizational change is one of the most important but also challenging tasks [Mo01, NJM02]. The organizational information security structure typically has to be adjusted to fit the identified regulatory requirements. The involved departments within security have to be identified, responsibilities and accountabilities for appointed tasks clarified as well as sender and receivers of consulting and information tasks defined where necessary. Especially regarding, but not limited to complex organizational structures, this is not trivial: To run an effective and efficient organizational change process, the executives need an integrated approach which supports the definition of the target state of the IS organization according to IS compliance, the identification of the current organizational structure and management of the change process to achieve the defined status.

An approach for these challenges is presented in this contribution. After introducing the RACI-model for assessing the current state of the information security organization in chapter 2, compliance principles are derived from IS requirements and combined with the RACI-model in chapter 3 to define the target state for an IS organization. In the following chapter 4, a process-oriented approach for managing the organizational change process is designed. Hereby, five steps are presented to facilitate a systematic process.

The authors emphasize that the proposed approach implies the IS definition and scope of the ISO standards what covers technical as well as non-technical security aspects [IS05a, IS05b]. Additionally, they are stressing that this approach does not focus on the overall IS process efficiency – it focuses on the improvement of compliance performance exclusively. So in contrast to the typical goal of change management, this approach may even decrease the overall process efficiency.

## 2 Current state assessment of IS organization with the RACI-model

### 2.1 Introduction to the RACI-model

For the current state assessment and target state definition of an IS organization the use of the RACI-model is suggested and introduced below. The objective of the RACI-model is to clearly define the role of a department for every task [SE07]. Therefore, the acronym RACI represents abbreviations for the following different roles:

- The **responsible (R)** role actually completes the task. It is responsible for action or implementation. Responsibility can be shared. The degree of responsibility is determined by the accountable (A) role.
- The **accountable (A)** role is ultimately answerable for the task or decision.
- The **consulted (C)** role typically is a subject matter expert, who provides necessary information and further consultancy. It is a predetermined need for two-way communication. Input from the designated role is required.

- The **informed (I)** role needs to be informed after a decision or action is taken. They may be required to take action as a result of the outcome. It is a one-way communication.

For the proper use of the RACI-model, an understanding of all tasks is necessary. Therefore, a hierarchical representation of tasks and sub-tasks is recommended [GB03].

## 2.2 Example: Using the RACI-model to assess an IS organization

The use of the RACI-model can now be illustrated within an example that was derived from a practical experience by the authors in the context of a global telecommunication company. This experience has proven the usability of the given assessment approach. For this purpose, the context of information technology (IT) service continuity and its management process was selected [Kö07, Rö05, SWP02].

The objective of the IT service continuity management (IT SCM) process is to minimize IT risks related to availability issues [Rö05, WK07]. According to the IT Infrastructure Library (ITIL), the following three sub-tasks can be associated with the management process [IT05, OCG01]:

1. **Plan IT service continuity strategy:** Based on a business impact and risk analysis, an IT service continuity strategy is defined. This strategy aims at providing IT service continuity to critical business processes [Wi07].
2. **Implement IT service continuity measure:** Based on the IT service continuity strategy, technical and non-technical (e. g. insurance) measures are implemented. Additionally, training is provided to IT staff.
3. **Operate IT service continuity processes:** Regular tests are performed to ensure the effectiveness of the implemented measures. Furthermore, change management processes consider major IT or business process changes in order to update the IT service continuity strategy where necessary.

Based on the sub-task structure, figure 1 provides an overview.

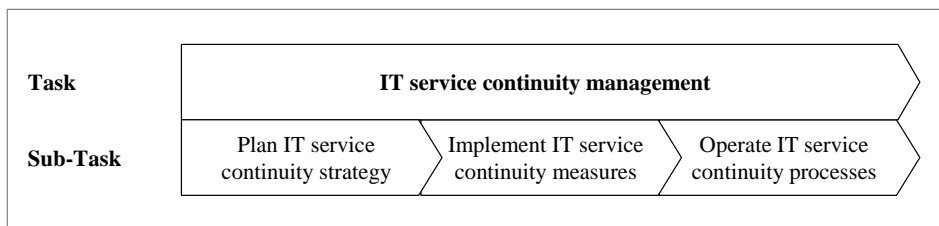


Figure 1: Tasks with IT service continuity management

To prepare the current state assessment, all involved departments within the IT SCM process have to be identified. COBIT therefore suggests 11 departments to take part

within IT SCM [IT05]. For illustrative purpose, a limited selection of the following 5 departments is suggested by the authors:

- The **business process department** describes the criticality of the relevant business processes and is responsible for the value-creation.
- The **IT management department** operates the IT systems to support the business processes. Therefore, it can provide insight about potential causes of IT risks. Moreover, it can suggest and implement preventive and reactive IT countermeasures.
- The **IS department** defines the IS concepts in order to protect the security objectives [FP00] like confidentiality, integrity and availability.
- The **risk management department** controls strategic and operational risks. Furthermore, it provides the methodology for risk management [Fi05].
- The **internal audit department** performs audits to validate the compliance to internal or external regulations.

In conclusion, table 1 shows the tasks and the involved departments.

	<b>Business process</b>	<b>IT management</b>	<b>IS management</b>	<b>Risk management</b>	<b>Internal audit</b>
<b>IT service continuity management</b>					
<b>1. Plan IT SC strategy</b>					
<b>2. Implement IT SC measures</b>					
<b>3. Operate IT SC processes</b>					

Table 1: Current state assessment

Based on the RACI-model, a role can now be assigned to the different departments for every task, in accordance to the current state of the IS organization. To perform the organizational assessment, all relevant and available documentation (e.g. organization plans) needs to be considered. Additionally, interviews and workshops assist in complementing the assessment.

### **3 Combining the RACI-model and compliance principles to define the target state for an IS organization**

#### **3.1 Compliance principles deducted from regulatory IS requirements**

The three IS standards ITIL, COBIT and ISO 27001 have been selected by the authors for the deduction of compliance principles. To prepare the analysis, the objective of the standards is summarized below [Bi06]:

- **ITIL** is a process based standard for IT service management. It contains best practices to improve effectiveness and efficiency within the IT organization.
- **COBIT** (Control Objectives for Information and related Technology) provides guidelines for IT governance. Therefore, it includes process goals and metrics.
- **ISO 27001** is a standard for the implementation of an IS management system and defines generic control objectives.

The standards only provide imprecise guidelines in the organizational context. For instance, in ISO 27001 the control requirement A.6.1.3 states that “all IS responsibilities should be clearly defined” [IS05b]. Therefore, an interpretation is needed in order to deduct specific compliance principles. The authors recommend aligning the compliance principles to the RACI-model as outlined below:

- **R-Principle:** Only a minimal number of departments should be responsible for each task.
- **A-Principle:** Only one department should be accountable for each task.
- **C-Principle:** Where necessary, complementary departments should be involved; e.g. business process departments can provide additional knowledge to business aspects within IT-related tasks.
- **I-Principle:** Where necessary, other departments should be informed; e.g. internal audit should be informed about strategic IT risk management decisions.

These principles form the baseline for the target state definition example.

### 3.2 Defining the target state of the IS organization – an example

The compliance principles and the RACI-model can now be used to define the target state of the IS organization within the example of IT service continuity management. According to the compliance principles, the guidelines within the relevant standards and the experience of the authors, roles are assigned for the example as shown in table 2.

	<b>Business process</b>	<b>IT management</b>	<b>IS management</b>	<b>Risk management</b>	<b>Internal audit</b>
<b>IT service continuity management</b>	A (1)	R	C	C	I
<b>1. Plan IT SC strategy</b>	A/R	C	C	C	I (2)
<b>2. Implement IT SC measures</b>	A/I	R (3)	-	-	-
<b>3. Operate IT SC processes</b>	A/R (4)	R	C	C	-

Table 2: Target state definition

Selected grey-shaded assignments and the rationale are illustrated below.

- (1) The business process department has to ensure that business processes create value for the enterprise. Therefore, the business risk owner also bears operational IT specific risks and is accountable for the overall process and its sub-tasks.
- (2) Internal audit examines the compliance assurance of the enterprise. It is informed about the IT service continuity strategy that has been decided by the business process department.
- (3) Measures within IT SCM are typically IT-based. Hence, the IT management department is responsible for their implementation.
- (4) The operation of the IT SCM process must include business and IT aspects. Therefore, both the business process and the IT management department are responsible.

For the target state definition, two critical success factors can be identified in the experience of the authors: Firstly, a top-down IS organization design should always agree upon roles at a higher task level with the leadership team. Afterwards, roles within sub-tasks can be specified. Secondly, the rationale of the assignment of roles to involved departments should be documented. This is especially important if an assignment differs from the typical guidelines of official standards. For instance, COBIT suggests that IT management should be accountable for the IT SCM process. If, as assumed above, the business process department is the overall risk owner, it is necessary to document the rationale.

## **4 Managing the organizational change using a process-based approach in order to improve information security compliance**

### **4.1 Introduction to a business aligned IS management concept**

In this chapter, a systematic management concept is introduced. This concept helps to develop a set of measures in order to achieve a defined IS target state in line with business needs and requirements [GL06]. Therefore, the concept of Business Aligned Information Security Management (BAISeM) can be applied and is introduced below.

BAISeM is part of an integrative framework for the entire business oriented information security management [KSST07]. It consists of two parts:

- **BAISeM rings:** While the outer ring contains the compliance requirements, the inner ring contains the strategic requirements. Both of them are derived from the individual contribution of the information processing processes and the overall business achievements.

- **BAISeM kernel:** A method for managing the IS requirements aligned to business goals and strategies is anchored in the kernel. It is based on the principles of the Balanced Scorecard [KN96c] as seen in diverse publications such as [BKZ06, KN96a, KN96b, KN05, SK01].

Using the BAISeM concept has several benefits:

- The concept supports the decision makers management of the IS requirements based on a transparent and balanced set of objectives, metrics and measures.
- Conformities and conflicts of IS objectives can be identified in order to handle the complexity of different IS requirements.
- Measures can directly, systematically and selectively be managed in order to reach the defined objectives using the metrics for controlling the achievement.
- The primary objective of securing the information infrastructure can be carried over to a hierarchical system of objectives and communicated within the enterprise.
- The hierarchical system can be used to get a top management overview over the IS management system filtered by strategic metrics. In addition, it can be used to monitor operating levels while slicing and dicing through the metrics system.

The examples show neither technical nor logical IS aspects but describe economic management issues that have been the rationale for the development of BAISeM [GL06].

Thereby, the concept uses a systematic process for aligning compliance requirements to the set of measures. This process is described in the next chapter concentrating on organizational issues.

## 4.2 Using the business aligned IS management concept in order to manage the organizational change process for IS compliance

Five steps are introduced in this chapter to manage the organizational change process regarding IS compliance as visualized in figure 2.

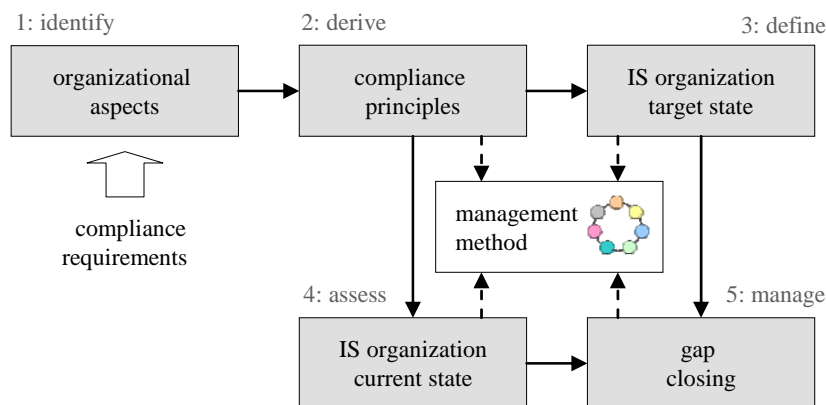


Figure 2: Process for managing compliance motivated organizational change

The steps are described below and the connection of each step to the central scorecard-based management method stressed individually.

1. **Identify:** In the first step, the IS relevant elements have to be separated from the overall range of compliance requirements the enterprise is confronted with. As discussed above, the standards ITIL, COBIT and ISO 27001 have been selected for illustrative purpose, with each of the standards containing various statements focusing on different sectors of IS. For instance, ISO 27001 lists requirements concerning policy, human resources security, physical and environmental security, communications and operations management as well as others [IS05b]. Similar and further aspects can be found in ITIL and COBIT.

*Result for illustrative purposes:* ISO 27001 requires in A.6.1.3 that “all IS responsibilities should be clearly defined” [IS05b].

*Link to management method:* There is no direct link to the BAISem kernel.

2. **Derive:** In the second step, compliance principles have to be assigned. As stated in chapter 3.1, these principles are used as a baseline for the target state definition. Therefore, they are of severe importance although the suggested set is defined as simple as possible in order to ensure minimal practical complexity regarding its usage in the management context.

*Result for illustrative purpose:* Set of RACI-principles as described in chapter 3.1.

*Link to management method:* The compliance principles are used as a development guideline for the set of metrics with which the achievement of IS compliance is monitored [Kü03]. While concentrating on the process perspective, the authors point out that the metrics themselves are not within the scope of this contribution.

3. **Define:** To define the target state of the IS organization, the RACI-principles of step two are linked to the RACI-model in the third step.

*Result for illustrative purpose:* Target state definition according table 2, showing that the internal audit must be informed about the IT SC strategy.

*Link to management method:* The target state definition table is transferred to the scorecards' objective attributes.

4. **Assess:** In step four the current state of the IS organization is assessed. The RACI-model may be used while the analysis of relevant documentation for instance, as well as interviews or workshops, can help to fill the table of the model.

*Result for illustrative purpose:* Current state assessment according to table 1 (but filled with results of the individual assessment), showing that the internal audit is not informed about the IT SC strategy.

*Link to management method:* The current state definition table is linked to the scorecard and compared with its objective attributes in order to derive the gaps to close. In this context the fourth step of the process leads to the assignment of the starting points of necessary measures for organizational change.

5. **Manage:** Closing the gap between the current and target state of the IS organization is the subject of matter of step five. Therefore, measures are developed in order to close the identified gaps. They are implemented and their achievement is monitored.

*Result for illustrative purpose:* The documentation of the IT service continuity strategy is sent to the internal audit department. A process for informing the department in cases of strategy changes is defined.

*Link to management method:* The measures are documented in the scorecard and monitored by the defined metrics. Thereby, the indicators of the metrics support executives to concentrate on those measures which are perceived as the most important ones. The status of achievement is visualized.

While managing the measures of the change process, BAISeM can be used to control this change process in order to improve the measures effectiveness. While the primary objectives are derived from the compliance requirements using a manual analysis process or relying on the information provided by the legal affairs division for instance, the central multi-dimensional scorecard system should use the data extracted from the current and target state assessment as described above as input variables. Combined in a organizational dimension and linked to other scorecard elements through cause-effect-chains, BAISeM enables to visualize the organizational IS gaps transparently. Moreover,

it gives an insight into the relationship between organizational IS aspects and other security measures as well as it supports the process of communicating the necessity for additional initiatives respectively for optimizing currently implemented measures to the IS concerned departments. Due to the extracted knowledge about different gaps and its relationships, suitable measures can be optimally implemented respectively revised. Against this background, BAISeM strongly supports the objective of improving the overall IS compliance.

As a result, not only IS compliance management but IS compliance performance management can be achieved. Additionally, the IS management activities can be easily documented. This is an important aspect for security certification.

## **5 Conclusion**

The key outcome of this contribution is an approach that systematically supports the management of organizational change and helps to improve organizational IS compliance.

In this context, the RACI-model was introduced to assess the current state as well as to define the target state of the IS organization. Later, a process-oriented management approach for assuring the systematic organizational change process was developed. Within this process, the RACI-principles derived from requirements were used as a baseline for the definition of the target state of an IS organization. It was addressed that for controlling purposes, the result should be transferred to objectives anchored in the IS scorecard of the BAISeM approach. As an example, a main compliance principle is the required implementation of appropriate organizational departments that are fully accountable (A) to a specific task in the IS context. This does not automatically imply that these departments also execute the related work tasks themselves but that other roles (R, C, I) are predefined.

The main benefit of the introduced approach can be seen in the support of the organizational change process with regard to the improvement of information security compliance. It enables the enterprise to get a transparent insight into the organizational state which has to be adjusted to better align the IS organization to the specific compliance requirements. Thus, an optimal set of measures for the change process can be developed. Additionally, the efficiency of the measures can be improved using metrics. Last but not least, the presented approach can help to document organizational IS compliance to prepare security certification.

Several associated other topics can be identified for further research, such as the development of the set of metrics. This is both a challenging as well as a highly specific task, for which reason the metrics themselves are not regarded in this contribution. Additionally, other use cases of the process could be analyzed, for instance a general IS maturity assessment or an IS auditing process.

## References

- [Bi06] BITKOM: Kompass der IT-Sicherheitsstandards, Leitfaden und Nachschlagewerk, Stand Juni 2006, Version 2.0, Berlin 2006.
- [BKZ06] Bible, Lynn; Kerr, Stephen; Zanini, Michael: The Balanced Scorecard: Here and Back. In: Management Accounting Quarterly, Vol. 7, No. 4, 2006; 18-23.
- [CA06] CA: IT-Sicherheit 2006/2007, Herausforderung Compliance, Eine Studie von CA, Analysen und Kommentare von Kuppinger Cole + Partner, Oktober 2006.
- [Ec05] Eckert, Claudia: IT-Sicherheit, Konzepte – Verfahren – Protokolle. München 2005.
- [Fi05] Fiege, Stefanie: Risikomanagement- und Überwachungssystem nach KonTraG - Prozess, Instrumente, Träger, Wiesbaden 2006.
- [FP00] Federrath, Hannes; Pfitzmann, Andreas: Gliederung und Systematisierung von Schutzziele in IT-Systemen. In: DuD, Datenschutz und Datensicherheit, 24. Jg., Nr. 12, 2000; 704-710.
- [GB03] Gabriel, Roland; Beier, Dirk: Informationsmanagement in Organisationen, Stuttgart 2003.
- [GL06] Gordon, Lawrence; Loeb, Martin: Managing Cybersecurity Resources – A Cost-Benefit Analysis, New York et al. 2006.
- [IS05a] ISO/IEC 17799: Information Technology – Security Techniques – Code of Practice for Information Security Management, ISO/IEC FDIS 17799:2005(E), Geneva 2005.
- [IS05b] ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements, ISO/IEC 27001:2005(E). Geneva 2005.
- [IT05] ITGI: COBIT -- Control Objectives for Information and Related Technology, Version 4.0, IT Governance Institute, 2005.
- [KN05] Kaplan, Robert, Norton, David: The Balanced Scorecard: Measures That Drive Performance. In: Harvard Business Review, Vol. 83, No. 7/8, 2005; 172-180.
- [KN96a] Kaplan, Robert, Norton, David: Balanced Scorecard: Translating Strategy into Action. Boston 1996.
- [KN96b] Kaplan, Robert, Norton, David: Linking the Balance Scorecard to Strategy. In: California Management Review, Vol. 39, No. 1, 1996; 53-79.
- [KN96c] Kaplan, Robert, Norton, David: Using the Balanced Scorecard as a Strategic Management System. In: Harvard Business Review, Vol. 74, No. 1, 1996; 75-85.
- [Kö07] Köhler, Peter: ITIL – Das IT-Service-Management Framework, 2. Aufl., Berlin/Heidelberg 2007.
- [KSST07] Klempt, Philipp; Schmidpeter, Hannes; Sowa, Sebastian; Tsinas, Lampros: Business Oriented Information Security Management – A Layered Approach. In: Proceedings of the 2nd International Symposium on Information Security (IS'07), Vilamoura 2007; 1835-1852.
- [Kü03] Kütz, Martin: Kennzahlen in der IT, Werkzeuge für Controlling und Management, 1. Aufl., Heidelberg 2003.
- [Mo01] Mott, Bernd: Organisatorische Gestaltung von Risiko-Managementsystemen, in: Gleißner, Werner; Meier, Günther (Hrsg.): Wertorientiertes Risiko-Management für Industrie und Handel - Methoden, Fallbeispiele, Checklisten, Wiesbaden 2001; 111-137.
- [Mü05] Müller, Klaus-Rainer: Handbuch Unternehmenssicherheit, 1. Aufl., Wiesbaden 2005.
- [NJM02] Noor, Iqbal; Joyner, Terry; Martin, Robert: Challenges of Implementing Risk Management Processes, in: AACE International Transactions, 2002.
- [OCG01] OCG: Service Delivery, Version 2.5, The Stationary Office, London 2001.
- [Re02] Reimann, Konrad: Position of the "Internal Audit Department" in a BCP Project, in: Wiczorek, Martin; Naujoks, Uwe; Bartlett, Bob (Hrsg.): Business Continuity, Berlin/Heidelberg 2002, 64-79.
- [Rö05] Rössing, Rolf von: Betriebliches Kontinuitätsmanagement, 1. Aufl., Bonn 2005.

- [SE07] Smith, Michael; Erwin, James: Role & Responsibility Charting (RACI), Online: [http://www.pmfforum.org/library/tips/pdf\\_files/RACI\\_R\\_Web3\\_1.pdf](http://www.pmfforum.org/library/tips/pdf_files/RACI_R_Web3_1.pdf), abgerufen am 17. Mai 2007.
- [SK01] Sim, Kim Ling; Koh, Hian Chye: Balanced Scorecard: A Rising Trend in Strategic Performance Measurement. In: Measuring Business Excellence, Vol. 5, No. 2, 2001; 18-26.
- [SWP02] Schettler, Heinrich; Wieczorek, Martin; Philipp, Michael: Operational Risk and Business Continuity: An essayistic Overview, in: Wieczorek, Martin; Naujoks, Uwe; Bartlett, Bob (Hrsg.): Business Continuity, Berlin/Heidelberg 2002; 1-31.
- [Wi07] Wiedemann, Jochen: Quantitative Wirtschaftlichkeitsbetrachtungen für IT-Notfallmaßnahmen, in: Horster, Patrick (Hrsg.): D-A-CH Security 2007; 507-518.
- [WK07] Werners, Brigitte; Klempt, Phillip: Management von IT-Risiken in Supply Chains, in: Vahrenkamp, Richard; Siepermann, Christoph (Hrsg.): Risikomanagement in Supply Chains - Gefahren abwehren, Chancen nutzen, Erfolg generieren, Berlin 2007; 287-300.