FEATURE ARTICLE: IT SECURITY MANAGEMENT

Improving Transparency and Efficiency in IT Security Management Resourcing

Knut Haufe
PwC Cybersecurity Services

Srdan Dzombeta
PwC Cybersecurity Services

Knud Brandis
PwC Cybersecurity Services

Vladimir Stantchev
SRH University Berlin

Ricardo Colomo-Palacios
Østfold University College

The authors propose a resource management process for information security management systems to more transparently plan and assign costs of controls. The process relies on and is compliant with international standards of the ISO/IEC 27000 family and can be implemented by all organizations regardless of type, size, or nature.

Nearly all organizations today depend on appropriate secure and compliant information processing. This has been stated practically in relevant standards and frameworks as well as in the literature.[1,2] Furthermore, there is a growing consensus that such standards need to be properly operationalized with unequivocal policies, processes, and metrics.[3] Standards for the management of information security have been developed and established, with those devoted to the development and operation of an information security management system (ISMS) published in the ISO/IEC 27000 series.[4,5]

IT governance, although recognized as an important topic in academic and professional environments, often is not a top priory of executive management.[6,7] In this scenario, commoditization and novel technology delivery models such as cloud computing[8] often lead to an increase in the number of IT stakeholders, making IT governance even more complex. This environment requires novel governance models such as participatory and shared governance.[9] These developments make the planning, implementation, and maintaining of ISMS processes and controls even more costly, keeping in mind that information security and data protection are traditionally considered to be cost drivers. Security projects have often been justified on fear, uncertainty, and doubt.[10] Over the past few years, cost-benefit discussions have influenced information security

Published by the IEEE Computer Society
1520-9202/18/$33.00 ©2018 IEEE

practice.[11] The value of information must justify protection and personnel costs and—particularly in the context of shared, participatory governance—this justification must be even clearer.[12] Adjustment and cost-effectiveness are key elements of cost governance and prerequisites for a successful ISMS,[13–16] while adequate funding of ISMS processes and controls is important and necessary to reach ISMS objectives.

ISMS budgets are often stressed, and additional funding is often requested to implement necessary controls. However, in many cases controls are not realized due to budget problems. Often, it is assumed that controls are paid for from the ISMS budget. This results in a nontransparent and irrational allocation of costs. Instead, costs should be divided among the individual cost centers according to the information security requirements. As a prerequisite for this, an adequate differentiation between costs for specific controls and costs for running and maintaining the ISMS processes is necessary. Such a differentiation would allow the ISMS to assign costs for controls to the owners whose assets determine information security or data protection requirements.

This problem is still relevant and unsolved because in the current standards, there is no clear differentiation between ISMS processes and controls. For instance, ISO/IEC 27002 contains several controls regarding information security incident management and information security reviews, which are ISMS processes and not controls.[5] Available methods (such as ROI and ROSI) to decide how much to invest in security and privacy are not generally accepted because of their complexity.[17] To address this open research question, we propose a resource management process for information security management systems to more transparently plan and assign costs of controls. The proposed process relies on international standards of the ISO/IEC 27000 family and is compliant with them. The proposed process can be implemented by all organizations regardless of type, size, or nature.

STATE OF THE ART IN INTERNATIONAL STANDARDS

ISO and IEC formed a joint technical committee (ISO/IEC JTC 1) for experts to come together to develop worldwide information and communication technology (ICT) standards for business and consumer applications. The subcommittee SC 27 has a working group (WG 1), which develops and facilitates international standards for ISMSs. ISO/IEC 27001, as the international standard from ISO/IEC JTC 1 SC 27 WG 1 for ISMSs, is the security standard in enterprises.[4,18]

ISO/IEC 27001 contains the requirements for planning, implementing, operating, and improving an ISMS. Requirements are formulated in a general manner to fit all organizations independent of their size, objectives, business model, location, and so on. Absolutely no requirements are formulated for any specific technology in ISO/IEC 27001,[19] but the standard contains requirements for ISMS core processes.

The ISO/IEC 27000 series does not consist only of 27001. The second common standard for information security in the 27000 series is 27002, which contains the controls that should be implemented with an ISMS.[5] 27002 is linked with 27001 with an annex of 27001 listing the controls of 27002. Further standards of the 27000 series are as follows.

- 27000—Information Security Management Systems
- 27003—Information Security Management Systems—Guidance
- 27004—Information Security Management—Monitoring, Measurement, Analysis, and Evaluation
- 27005—Information Security Risk Management
- 27006—Requirements for Bodies Providing Audit and Certification of Information Security Management Systems
- 27007—Guidelines for Information Security Management Systems Auditing
- 27008—Guidance for Auditors on Information Security Controls
- 27010 and following—Information Security Management for Intersector and Interorganizational Communications
- 27030 and following—Standards for Technical Controls and Guidelines for Controls of ISO/IEC 27002

According to ISO/IEC 27000/27001, an ISMS process (which needs to be designed) is the resource management process, which ensures that necessary resources are determined and provided.[6] Nevertheless, no further information on how to define or establish such a process is provided in the standards.

The information security risk treatment process[4] is a process to select and implement controls to mitigate risk.[20] Controls are determined during the process of risk treatment, rather than being selected from Annex A of ISO/IEC 27001 (see www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Processes-product-page.aspx).

THE PROCESS

Governance deals with value delivery to the stakeholders, risk optimization, and resource optimization (see www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf). Governance is also the responsibility of executives and boards of directors, and consists of the leadership, organizational structures, and processes that ensure that the organization's strategies and objectives are reached.[21] As leadership, risk assessment, risk treatment, and resource management are elements of the ISO/IEC 27001, the concept of cost governance in IT security management is integrated in ISO/IEC 27001.[4] Here, we focus on the proposed resource management process as part of cost governance in IT security management.

The resource management process is the process to identify, allocate, and monitor required resources to run the ISMS core processes, as well as to implement and run the selected controls. So, a resource management process is key to efficiently use limited resources as part of the governance of IT security costs.

A resource management process is also part of the ISMS planning process. However, we focus on the management process for the resources necessary to operationally run the ISMS or security controls.

The resource management process needs to be carried out on a regular basis because it is integrated in the ISMS and continuously supports the ISMS processes as well as the controls by identifying, allocating, and monitoring the required resources. So, this is not a one-time task.

Table 1 and Figure 1 contain a description of the proposed process.

Table 1. Resource management process description.

Process name	Resource management process
Process categorization	Information security management system (ISMS) core process
Brief description	The resource management process identifies, allocates, and monitors required resources to run the ISMS core processes and to implement and run the selected controls. It enables the governance of costs for IT security management.
Objectives/purposes	Ensure that the resources for the ISMS and the controls are available Appropriate management of ISMS resources Ensure efficiency of resource usage
Input	From risk treatment process: drafts and final list with selected controls From ISMS planning project: management approval for initiating the ISMS and documented business case for the ISMS/project proposal

	From purchasing department: list of suppliers, framework contracts, and terms and conditions of purchasing
Output	For information security risk treatment process: estimation of necessary resources to implement controls For communication process: estimation of necessary resources to operate the ISMS core processes and reports regarding resource usage of ISMS core processes For information security customer relationship management process: reports on resource usage
Activities/functions	Initially plan necessary resources to implement and run the controls Categorize controls: a differentiation is made between controls funded by the ISMS budget and controls funded by other departments Communicate necessary resources to the information security risk treatment process to implement and run the controls; if necessary, repeat this step and the planning of necessary resources Communicate necessary resources to the communication process regarding the ISMS controls (necessary to operate the ISMS core processes) Allocate necessary resources for approved controls funded by the ISMS Permanently monitor ISMS resource usage, and, if necessary, update resource allocation Develop and communicate reports regarding resource usage of ISMS core processes to the information security officer (ISO)
Sample metrics	Key goal indicators: Count of activities/functions of the ISMS that were not performed due to a lack of resources Key performance indicators: Resources to implement the selected controls Planned but not used resources and resource trends Count of controls with budget overrun Ratio between ISMS-funded controls and otherwise-funded controls
Owner	ISO
Manager	ISO or resource manager
Actors	ISO or resource manager Purchase and human resources department Consultants and specialists
Interfaces	This process is interlinked with the information security risk treatment process and all other ISMS core processes as well as processes of the purchasing and human resources departments.

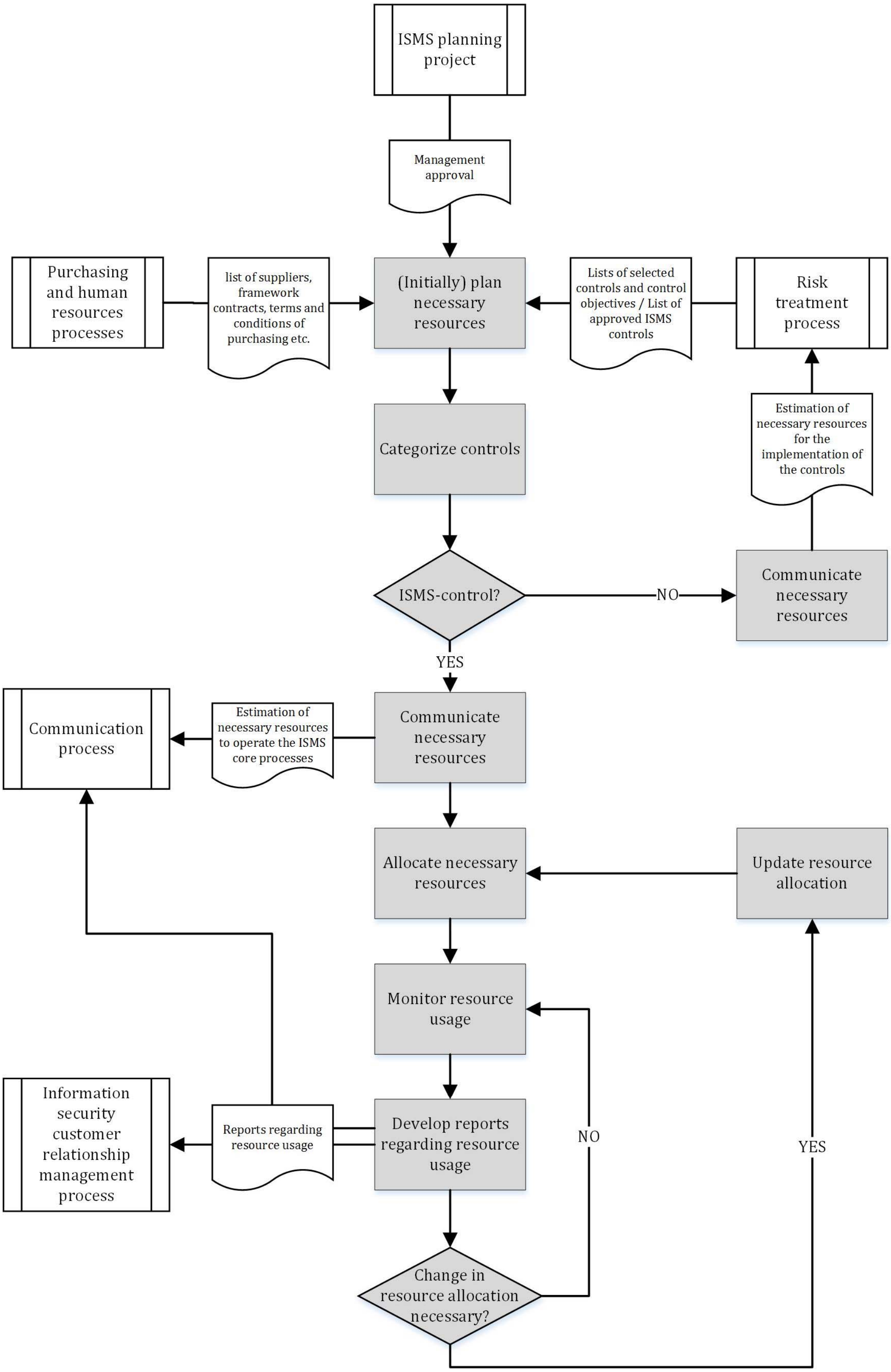
ISMS planning project
Management approval
Purchasing and human resources processes
list of suppliers, framework contracts, terms and conditions of purchasing etc.
(Initially) plan necessary resources
Lists of selected controls and control objectives / List of approved ISMS controls
Risk treatment process
Categorize controls
Estimation of necessary resources for the implementation of the controls
ISMS-control?
NO
Communicate necessary resources
YES
Communication process
Estimation of necessary resources to operate the ISMS core processes
Communicate necessary resources
Allocate necessary resources
Update resource allocation
Monitor resource usage
Information security customer relationship management process
Reports regarding resource usage
Develop reports regarding resource usage
NO
YES
Change in resource allocation necessary?

Figure 1. Resource management process flow chart.

Key to the proposed resource management process is the categorization of controls that must be funded by the ISMS and controls that should be funded by other departments.

The ITIL framework[21] integrates the idea to charge costs for IT services to the functional units that use IT services. Considering this idea, it sounds obvious to charge costs for information security measures to the functional units demanding those measures. To realize this, a clear differentiation should be made between ISMS processes financed by the chief information security officer (CISO) and other security measures financed by other cost centers. As a result, information security costs are made transparent and can be better managed.

We propose using this categorization as the main criterion to differentiate controls funded by the ISMS and controls funded by other departments. Only ISMS core processes should be financed by the ISMS. All other controls should be charged to functional units, departments, or cost centers demanding those controls.

Core processes deliver apparent and direct customer value and are derived from the core competencies of an organization. From the perspective of the ISMS, a core process is the core competency of the ISMS and delivers apparent and direct value to the stakeholder (generally the organization implementing the ISMS and the management of the organization).

ISMS core processes are operational processes that need to be repeated regularly.

Thinking about processes in general as well as ISMS processes means asking what needs to be done on a regular basis.[22] Therefore, ISMS core processes are operational processes (mainly, but not limited to, part of the "Do" and "Check" steps of the PDCA cycle) that need to be repeated regularly. Furthermore, a criterion for the categorization as an ISMS core process is that the process is owned by the information security officer (core competency of the ISMS). This means that the information security officer is accountable for the whole process and defines objectives and goals for the process derived from the objectives of the ISMS, which will be defined by senior management. In many practical cases, especially in small organizations, the information security officer will also be the process manager responsible for the process operation. This could also be used as a criterion for ISMS core processes.

We propose the following basic criteria to identify ISMS core processes.

1. Regularity—interrelated and interacting tasks are repeated on a regular basis.
2. Transformation—inputs are transformed into outputs.
3. Operation—process is carried out while operating the ISMS.
4. Accountability/responsibility—the information security officer is the process owner or process manager and the process is a core competency of the ISMS.
5. Value generating—delivers apparent and direct value to the stakeholder.

All criteria must be fulfilled to qualify a process as an ISMS core process. Criteria 1 and 2 are basic criteria to identify processes, but they are necessary to exclude one-time tasks like obtaining management's commitment to establish an ISMS or tasks within a process. Criterion 3 is mainly a basic process criteria, but is necessary to exclude processes that are not part of the operation of the ISMS. An example is the initial ISMS planning process, which is carried out during the ISMS planning phase. Criterion 4 is the main criteria to decide whether the process is ISMS-owned and requires ISMS core competencies. Criterion 5 is necessary to exclude supportive processes like the documentation and records control process from the ISMS core processes.

These criteria should not be used in a binary way (fulfilled or not fulfilled). Instead, the level of fulfilment of a criterion (for example, how much value is generated by the process) should be used to discuss and decide whether the process can be understood as an ISMS core process.

EVALUATION RESULTS

The proposed resource management process was implemented as a pilot project in a software development company specializing in healthcare. The company is located in Germany (one main office and an additional branch office), has a staff of 50, and uses an outsourced datacenter.

Altering the resource management process was part of a project to implement ISO/IEC 27001 compliance. A preliminary project to implement an ISMS had failed the year prior to the new project (budget for external consultants: 60 person days). From our viewpoint, the main reason for this was that the ISMS project tried to compensate for unavailable information within the project budget. For example, in the failed project it was identified that the IT documentation was out of date and incomplete, so about 20 person days from the project budget were spent to gather information about the IT. This not only unnecessarily reduced the limited project budget, but it was also unsustainable because the reason for the inappropriateness of the documentation was not discovered.

IT documentation and the change-management process were not part of the new ISMS project. We also recognized a strong barrier from the IT staff when they were only told that the IT documentation was not appropriate, what the requirements were, and that they needed to solve the problem within the IT budget. We needed to communicate additional requirements and to convince management and every administrator why it is necessary and beneficial (for every individual) to maintain appropriate IT documentation.

The existing risk-management processes were altered to integrate interfaces for the new process, which was not in place at all. The company had no idea what it cost to operate an ISMS because costs for security controls were not differentiated. Another main challenge of the new process was that not all risk-treatment options and security controls were approved by the information security officer. In the new process, the risk owner is generally accountable for deciding how to mitigate the risk. This is not new, but the clear differentiation between general security risks (mitigated within ISMS core processes) and specific security risks outside the ISMS (such as inappropriate IT documentation) helped focus the ISMS budget on the establishment and operation of the ISMS.

The main challenge regarding resource-usage monitoring within the ISMS was to identify significant metrics like time spent for risk analysis and to continually gather the necessary data for those metrics. The company is still improving this ISMS resource-usage monitoring. It was also difficult to include processes with a low maturity level in the resource-usage monitoring. The company decided to implement an information-security-awareness process at a repeatable maturity level because they felt that all employees were highly skilled. So, they focused on informal and ad-hoc awareness measures instead of planned, documented trainings. Gathering resource usage data for processes like this is still a challenge for the company.

The new resource management process is now in place and has been operating for six months at the time of this writing. During this time, feedback from senior management and the information security officer was gathered continually during formal meetings and informal discussions.

From the viewpoint of senior management, two main advantages of the new process were recognized compared to the former processes.

1. More transparency of information security costs. Due to the separation of costs for the ISMS and costs for individual controls, senior management feels better informed about the use of resources for information security. This also positively influences discussions about security controls among management, departments, and the information security officer.
2. Improved decision making. Senior managers feel more confident in the decision-making process regarding information security controls and have a better understanding of where costs are coming from.

From the viewpoint of the information security officer, two main additional advantages of the new resource management process were recognized compared to the former processes:

1. Improved image. Because of the transparency of cost allocation, information security is no longer recognized as a global cost driver. This objectifies budget discussions.
2. Improved efficiency. Time spent for budget discussions was dramatically reduced. Because of the clear differentiation of ISMS costs and costs for controls, the information security officer no longer had to fight for budget for the controls aside from the ISMS core processes. Instead, this task was assigned to the business units. Also, nearly 90 percent of the security requirements gathered in the failed project were reduced due to the risk owner's new understanding that they needed to fund the security controls.

A direct measurement and comparison of the costs before and after implementing the new process is difficult because no process was in place when the project began and the ISMS itself was not complete.

CONCLUSIONS AND FUTURE WORK

The pilot implementation of the resource management process proved that a differentiation between costs for the ISMS and costs for individual controls can shift the image of information security from a cost driver to a transparent and manageable success factor. Furthermore, it provides a precise answer to the question, "Who owns IT?"[9] in the specific area of ISMSs. IT governance can be improved by the process as it provides cost transparency even in complex shared or participatory governance settings.

Future work is envisioned in three main steps:

- Further evaluation of the proposed process. Results of the evaluation of the resource management process will be analyzed empirically. Changes and consequences of implementing the process must be specifically measured to allow a more reliable evaluation of the process. Consequences for the long-term budgets for ISMS and information security controls are of special interest.
- Development of an ISMS core process framework. To the best of our knowledge, there is not a specific process framework for security management that clearly differentiates between ISMS processes and the security measures controlled by ISMS processes. Furthermore, a detailed description of ISMS processes and their interaction as well as the interaction with other management processes does not exist. This ISMS process framework should be developed and data across industries should be gathered to demonstrate the viability and effectiveness of the proposed framework.
- Development of a method to adjust and make costs transparent for operating the ISMS core processes. Transparency of information security costs could be further improved by tailoring the maturity level of ISMS processes to the requirements of the organization. Assuming that not every ISMS process needs the same level of maturity, an approach should be developed to identify the appropriate level of maturity using a proper maturity model. This model, together with the specific assessment tools to determine the appropriate maturity model for an organization, will optimize information governance costs. Furthermore, costs can be attributed properly to specific services with respect to their configuration[23] and thus provide more transparent cost information in the marketplace for cloud services.[24]

REFERENCES

1. F. Holik et al., "Methods of Deploying Security Standards in a Business Environment," *Proc. 2015 25th Int'l Conf. Radioelektronika* (RADIOELEKTRONIKA), 2015, pp. 411–414.
2. M. Ndungu and S. Kandel, "Information Security Management in Organizations," dissertation, Centria Univ. of Applied Sciences, 2015; www.theseus.fi/bitstream/handle/10024/96779/Thesis_maryanne_sushila.pdf.

3. S. Earley, "Information Governance in the Age of Big Data: IT Professional Conference on Challenges in Information Systems Governance," *IT Professional Conference* (IT PRO), 2014; ieeexplore.ieee.org/abstract/document/7029281.
4. *ISO/IEC 27001:2013, Information Technology—Security Techniques—Information Security Management Systems—Requirements*, standard ISO/IEC 27001:2013, ISO/IEC, 2013.
5. *ISO/IEC 27002:2013, Information Technology—Security Techniques—Code of Practice for Information Security Controls*, standard ISO/IEC 27002:2013, ISO/IEC, 2013.
6. S.J. Andriole, "Boards of Directors and Technology Governance: The Surprising State of the Practice," *Comm. Assoc. for Information Systems*, vol. 24, 2009, pp. 373–394.
7. T. Lucio-Nieto et al., "Implementing an IT Service Information Management Framework: The Case of COTEMAR," *Int'l J. Information Management*, vol. 32, no. 6, 2012, pp. 589–594.
8. S. Dzombeta et al., "Governance of Cloud Computing Services for the Life Sciences," *IT Professional*, vol. 16, no. 4, 2014, pp. 30–37.
9. S.J. Andriole, "Who Owns IT?," *Comm. ACM*, vol. 58, no. 3, 2015, pp. 50–57.
10. M.S. Merkow and J. Breithaupt, *Information Security: Principles and Practices*, Pearson IT Certification, 2014.
11. Z. Tu and Y. Yuan, "Critical Success Factors Analysis on Effective Information Security Management: A Literature Review," *Proc. 20th Americas Conf. Information Systems* (AMCIS), 2014; pdfs.semanticscholar.org/aa02/0f53503050a6e53d6403c6aa48f5dcbc3b9c.pdf.
12. T. Coulson et al., "The Price of Security: The Challenge of Measuring Business Value Investments in Securing Information Systems," *Comm. IIMA*, vol. 5, no. 4, 2005; scholarworks.lib.csusb.edu/ciima/vol5/iss4/3.
13. M.H. Khyavi and M. Rahimi, "The Missing Circle of ISMS (LL-ISMS)," *Proc. 2015 ACM SIGMIS Conf. Computers and People Research* (SIGMIS-CPR), 2015, pp. 73–77.
14. Y. Ozdemir et al., "Evaluation and Comparison of COBIT, ITIL, and ISO27K1/2 Standards within the Framework of Information Security," *Int'l J. Technical Research and Applications*, no. 11, 2014, pp. 22–24.
15. Z. Tu, "Effective Information Security Management: A Critical Success Factors Analysis," dissertation, McMaster Univ., 2015; macsphere.mcmaster.ca/handle/11375/18168.
16. G. Chehrazi, C. Schmitz, and O. Hinz, "QUANTSEC—Ein Modell zur Nutzenquantifizierung von IT-Sicherheitsmaßnahmen," *Wirtschaftsinformatik 2015 Osnabrück*, 2015; pdfs.semanticscholar.org/9ea3/98e0dd9edd244211120abdad630737d3f0f4.pdf.
17. W. Boehmer, "Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001," *2nd Int'l Conf. Emerging Security Information, Systems, and Technologies* (SECURWARE), vol. 8, 2008, pp. 224–231.
18. J. Brenner, "ISO 27001: Risk Management and Compliance," *Risk Management*, vol. 54, no. 1, 2007, p. 24.
19. *ISO/IEC 27000:2014, Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary*, standard ISO/IEC 27000:2014, ISO/IEC, 2014.
20. D. Brewer, *Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013*, technical report, BSI Group, 2013; www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/BSI-ISO27001-transition-guide-UK-EN-pdf.pdf.
21. S. Taylor et al., *ITIL Version 3: Service Design*, technical report, Office of Government Commerce, 2007; tomjsmyth.files.wordpress.com/2015/04/itilv3sd-itil-v3-service-design.pdf.
22. N. Slack, S. Chambers, and R. Johnston, *Operations Management*, Financial Times/Prentice Hall, 2009.
23. H. Krallman et al., "Enabling Autonomous Self-optimization in Service-Oriented Systems," *Autonomous Systems—Self-Organization, Management, and Control*, Springer, 2008, pp. 127–134.
24. V. Stantchev and G. Tamm, "Reducing Information Asymmetry in Cloud Marketplaces," *Int'l J. Human Capital and Information Technology Professionals*, vol. 3, no. 4, 2012; www.irma-international.org/viewtitle/73709.

ABOUT THE AUTHORS

Knut Haufe is managing director and lead expert for information security management systems at PwC Cybersecurity Services. His research interests include process reference models, integrated management systems, and maturity levels. Haufe received a PhD in information technology from the Universidad Carlos III de Madrid. He is a member of the Standards Committee on Information Technology and Applications (NIA) 043-01-27-01 of the DIN (German Institute for Standardization). Contact him at khaufe@pwc-cybersecurity.com.

Srdan Dzombeta is a partner at PwC Cybersecurity Services. His research interests include internal control systems and cloud systems. Dzombeta received a PhD in information technology from the Universidad Carlos III de Madrid. Contact him at sdzombeta@pwc-cybersecurity.com.

Knud Brandis is a partner at PwC Cybersecurity Services. His research interests include information security and risk management. Brandis received an MBA in financial management from the University of Wales. Contact him at kbrandis@pwc-cybersecurity.com.

Vladimir Stantchev is the executive director of the Institute of Information Systems at SRH University Berlin, where he is also a research professor. He is also a professor at the University of Granada and an affiliated senior researcher with the Networking Group at the International Computer Science Institute (ICSI). Stantchev's research interests include IT governance, cloud computing architectures, IT strategy, and methods for service and software engineering. He received a PhD in system architectures from the Berlin Institute of Technology. Stantchev is a Senior Member of the IEEE Computer Society and ACM. Contact him at stantchev@computer.org.

Ricardo Colomo-Palacios is a full professor in the Computer Science Department at Østfold University College. His research interests include applied research in applied information systems including IT governance and service management. Colomo-Palacios received a PhD in computer science from the Universidad Politécnica of Madrid. Contact him at ricardo.colomo-palacios@hiof.no.