Information Security Risk Management in Higher Education Institutions: From Processes to Operationalization

Wolfgang Hommel[1], Stefan Metzger[2], Michael Steinke[3]

[1]Leibniz Supercomputing Centre, Garching n. Munich, Germany, wolfgang.hommel@lrz.de
[2]Leibniz Supercomputing Centre, Garching n. Munich, Germany, stefan.metzger@lrz.de
[3]Leibniz Supercomputing Centre, Garching n. Munich, Germany, michael.steinke@lrz.de

Keywords
Information security, Risk management, ISO/IEC 27001, Higher education data center

1. ABSTRACT

Information security has successfully gained high levels of management attention in European higher education institutions (HEIs) over the past decade, but is the data stored in HEI data centers, IT departments, or faculty server rooms really more secure as a consequence? In this article, we first review how information security policies and risk management processes were typically introduced in HEIs as an important first step, but then argue that many HEIs still need to complement these "people and processes" steps with efforts to make efficient use of them on the "technology" layer.

HEI servers that can be accessed from the public Internet have a long history of being lucrative targets for attacks by all kinds of miscreants because, e.g., the network bandwidth available at many HEIs can be misused for sending Spam emails or participating in high-volume denial-of-service attacks. More targeted attacks are performed, e.g., to spy on intellectual property related to research projects and HEI collaborations with industry partners. And in times of *doxing*, i.e., the black-hat hacker sport of making an organization's internal documents and emails public, as in the 2014 Sony case, the demand for protecting certain data even against more determined attackers become obvious. Until about 10 years ago, most system administrators and service operators were sufficiently familiar with the information security implications of the hardware and software in their area of responsibility. But meanwhile, services such as private cloud hosting environments, groupware collaboration tools, and web-based learning management systems have grown to a complexity that practically cannot be mastered by individuals anymore. More often that not, complex software services are operated in production use without scrutiny regarding their security settings or thorough consideration of additional security measures that should be placed upstream.

To cope with this increase in complexity in a structured manner, security management processes, e.g., based on the international ISO/IEC 27001 standard, have been introduced, along with the assignment of responsibilities to roles such as HEI Chief Information Security Officers (CISOs), the preparation of policies, e.g., regarding data classification and secure disposal of media, and check lists for handling security incidents and data breaches efficiently. According to the textbooks and for very valid practical reasons, risk management drives each of these activities.

However, information security risk management is a process that requires a lot of information as input, and even more expertise. It can therefore quickly turn into a useless placebo paper tiger when it is not applied properly in practice. But when given only a high-level process description, many system administrators and service managers do not know how to do risk management in a meaningful way, i.e., with reasonable efforts and immediate benefits from the results. We therefore present our strategy for *operationalizing information security risk management* in a HEI data center with a focus on both HEI-internal IT services as well as HEI cooperation, e.g., in research projects, with the long-term goal of compiling the feedback we receive into a HEI best practice guide on information security risk management.

2. INFORMATION SECURITY: TOOLS OF THE TRADE

In order to understand the strengths and weaknesses of information security risk management in HEIs as of today, it is important to know how information security has developed as a discipline and what HEIs have done to jump on the bandwagon. Just like many other areas of information and communication technology, information technology started as an almost purely technical field of action. This era, which we summarize shortly in Section 2.1, has brought many great methods and tools, most of which are as important as ever, but having a system administrator's head trapped in this mindset can cause more harm than benefit today. Good practices for IT service management, as they became popular with frameworks like ITIL® and standards, such as ISO/IEC 20000-1, provide the big picture for offering and operating IT services in a customer-oriented manner and include information security management as one of their pillars or cross-sectional processes. Because security management is most often seen as part of IT service management, we discuss the resulting implications in Section 2.2. Higher education was not the first sector to routinely have formal information security management introduced in an organization-wide manner, but meanwhile most HEIs of any size have an information security management system, consisting, e.g., of processes, policies, and role assignments set up and running. This constitutes our initial situation and is presented as an overview in Section 2.3.

2.1. The era of security technology without management as we know it today

Until about the mid-1990ies, information security was a riddle wrapped up in an enigma for most IT service users and the management; with a few exceptions, such as password-protected access to services and data, it went mostly unnoticed by everyone except the system administrators who had to fiddle about the inner workings of these services. Technical terminology that was heavily influenced by military wording, such as *attacks* and *demilitarized zones*, and technology associated with the military realm, such as *encryption*, added to the mystery. It stems from these times that a considerable portion of the technical IT staff still considers themselves alone as able and appropriate authority for anything related to information security and tries to maintain the somewhat paradox state of not being bound to outside directives while "voluntarily" taking on only a very limited personal responsibility in the case of information security catastrophes.

Following this golden era of little interest in and even less control of what the IT staff did IT-security-wise, management interest in information security started to rise under the guise of compliance: Organizations started to not only have to justify their steadily increasing IT expenses in more detail, but new laws which made very clear that information security shall not work without top-level management commitment.

2.2. Security management as a part of IT Service Management

Information security is not the only discipline that suffered from the growing complexity of IT infrastructures over the years in practice. Fulfilling user requests, fixing technical incidents and faults, and keeping track of inter-service dependencies are just a few examples of tasks that can easily be done on a small scale, but they need structured and often tool-supported workflows when growing in scale. Given the dozens of IT services provided by most HEI data centers, which often require hundreds servers and networking components that need to be maintained, constrained by a tight budget, especially for staffing, it comes at no surprise that increased efficiency through better policies, processes, workflows, and procedures is a charming option. Good practice documentations, such as the versions 2 and 3 of the IT Infrastructure Library (ITIL®), have started to attract a significant number of HEIs,and meanwhile the majority of HEI data centers uses them as guidance even if higher process maturity levels can take quite a long time to achieve. The basic merit of these good practice approaches is the description of individual processes, such as capacity management for planning resources ahead of time or release management including rollback option in case a software upgrade goes wrong; but their overvalue lies in the elaboration of the interdependencies between the individual processes, tasks, and people assigned to them. As will be discussed later in Section 3, security management is often designed as cross-cutting process with interfaces to almost any IT service management process, which ensures that information security is not only considered during the preparation of technical changes to the infrastructure, but also becomes an integral part of contracts made within the domain of service level management and configuration management.

Several IT service management processes can be turned into quick-wins, such as incident management, whose immediate benefits become obvious when, e.g., a trouble ticket system is set up and turns out to be a real time-saver for handling user requests and incident reports. Other processes, including security management, tend to have a harder start, because, among other factors, a lot of documentation such as various policies and process specifications (e.g., for security incident handling) has to be prepared. Writing those documents is often delegated to experts in the area, which means that people who are not yet fully convinced of the benefits of more formal processes and have a very technical background produce concepts, which run the risk of not striking the balance between being either too technical or too abstract to be useful for a broader audience. This potentially adds to the frustration of the technically oriented experts and seemingly proves that formal security management adds no real value but only wastes time.

What pundits often fail to recognize is, however, the important impact of a structured and extensive documentation of security management activities on the visibility from a top-level management perspective. As we will see in Section 5, the crux that needs to be climbed is assuring the technical staff of the necessity of formal methods and their turning to the staff's advantage at the same time.

2.3. Information security formalisms in higher education institutions

The extensive autonomy of organizational units in HEIs is often seen as a challenge for IT governance and security management is no exception. As shown in Section 3, management commitment to information security is one of the first important building blocks, and therefore many HEIs that, for example, established a chief information officer (CIO) position at the level of a vice president decide to introduce the role of a chief information security officer (CISO) either as a dual role for the CIO or appoint, e.g., the head of the IT department or a security expert in a leading position as CISO with direct reporting to the CIO.

Besides the formal responsibility that comes with the CISO position, it primarily is a boundary role between HEI management, IT service management and operations, the HEI-internal users, and inter-organizational special interest groups as well as public authorities, such as law enforcement. Due to the nature of this position, a CISO needs to set up an internal structure to ensure top-down and bottom-up information flow for all organizational units. One typical solution is to establish a HEI-wide information security working group with one representative, referred to as information security officer (ISO), from each department and central institution, e.g., the administration and the library.

Each represented organizational unit will have certain degrees of freedom to arrange internal sub-structures, which typically are required to assign further required security management roles closer to the staff level. These roles are, for example, related to risk management, asset and equipment management, disciplinary competence, physical and environmental security, access control, system and network security, and interfaces to other IT service management processes. As already this incomplete list makes obvious that a lot of dedicated tasks have to be performed, not yet including awareness programs and getting everyone actively involved in information security, such a HEI-wide working group can only give its attention to selected topics and therefore decision proposals need to be well-prepared by the individual organizational units. The key to both is to address the most important problems first, or, in other words, effective risk management, which is discussed in the next section.

3. INFORMATION SECURITY RISK MANAGEMENT: FRAMEWORKS AND TOOLS

There are numerous standards, frameworks, models and supporting tools available for risk management. Some of them are general-purpose and can be applied to any kind of risks, others addresses specific risks, e.g., financial, operational, strategic, or in particular IT risks. In this section a short-list of different, well-known and also internationally accepted risk management approaches focusing on information security risks will be presented.

Planning an information security management system (ISMS) based on ISO/IEC 27001 mandates a responsible handling of risks targeting the confidentiality, integrity, and availability of information or any other kind of critical assets, i.e., anything that has some value for an organization to accomplish its business objectives. In the context of the ISO27k standard series, ISO/IEC 27005 provides guidelines for information security risk management. Rather than specifying or giving some

recommendation and dictating specific risk management methods, the standard defines a continual risk management process consisting of a sequence of different activities. In the first step the risk management context has to be established, before threats and resulting risks have to be identified, assessed and dealt with. Some software tools support an ISO/IEC 27005 compliant risk management, e.g., the *SecureAware*[1] *ISMS tool* by Neupart or the open-source ISMS software *verinice*[2].

Another practically used risk management approach is provided by the German Federal Office for Information Security (BSI) and its standard documents BSI 100-X. The BSI's IT-Grundschutz Methodology also specifies an information security management process based on a more simplified risk management approach, which also starts with a structured analysis of the organization's ICT environment to derive security requirements. In contrast to ISO/IEC 27005, this methodology's best-practice orientation slashes the expended effort for threat and risk identification and their assessment through the definition of specific threat catalogues combined with catalogues describing appropriate security controls. In addition to that, if higher protection levels with relation to the assets' CIA requirements are needed or the ICT environment distinguishes from common operational scenarios, BSI's standard 100-3 provides the definition of a risk management procedure. Based on a threat analysis, which encompasses the IT-Grundschutz related threats, as well as the identification and assessment of additional threats, a suitable risk treatment has to be conducted. For this treatment, different options, e.g., reducing the risk by implementing specific security controls, risk avoidance, risk transfer, and acceptance are effective. Back to IT-Grundschutz methodology and its security process, a second security check has to be done after choosing an adequate risk treatment option to ensure that all remaining risks are acceptable by organization's top management.

Also the US-American National Institute of Standards and Technology (NIST) provides a risk management methodology defined in its special publication documents NIST SP 800-30 and NIST SP 800-39. In this approach, risk assessment is a key component of a holistic, organization-wide risk management process, which usually starts with a risk framing phase, i.e., analogously to ISO/IEC 27005 the establishment of an organization-specific risk management context and an appropriate strategy that addresses how the organization intends to assess and respond to identified risks. The risk assessment includes a risk model, which defines risk factors and their relationship to each other to determine risk levels. Typical risk factors are threats, vulnerabilities of an asset and impact, conditions, and constraints. A threat, its source, and the materializing risk for an asset are usually defined in so-called threat scenarios, which describe the events in more detail and how they contribute to cause harm. Uniquely NIST's risk assessment approach provides risk aggregation, which allows combination of singular low-level risks to more general or higher-level risks. Risk aggregation can also be used to describe relationships among discrete risks and the consequences, e.g., once one discrete risk materializes, another risk becomes more or less likely. NIST also deals with uncertainty to allow for limitations in exactly predicting the likelihood and the impact of a certain threat event. The risk management process itself consists of the identical phases as defined in ISO/IEC 27005.

Since a few years, besides the more generic risk management standards there exist more practicable approaches, methodologies and frameworks. The OCTAVE method – Operationally Critical Threat, Asset and Vulnerability Evaluation - was created to help organizations to perform information security risk assessments. The first version of OCTAVE, released about 15 years ago, focuses primarily on larger enterprises having a multi-layered organizational structure and are able to use vulnerability evaluation tools and interpret their results. OCTAVE as well as OCTAVE-S, an adapted version for use in smaller organizations, consist of three phases. In phase one, the organizational view is defined consisting of assets, threats, organizational vulnerabilities, and security requirements. Phase two provides a more technical view describing key components and their (technical) vulnerabilities. In the third phase the risks, the protection strategy as well as the mitigation plan are developed. In 2007, both versions were replaced by OCTAVE Allegro, which focuses primarily on information assets in the context of how they are used, where they are stored, processed, and transferred as well as exposed to threats, vulnerabilities, and any kind of disruption. The data collection process, which in previous OCTAVE versions was performed in workshops and by an analysis team, was replaced with a simplified worksheet-based method. It focuses on the

[1] http://www.neupart.com/products.aspx

[2] http://www.verinice.org

information itself as the asset worth protecting, so the definition of a risk management context is not mandatory anymore. IT systems, storage, and networking equipment as well as cloud infrastructure components used from service providers in outsourcing scenarios are defined as information asset containers. Within areas of concern, the analysis team describes threats in some kind of mostly unstructured way before they are expanded to threat scenarios to enable risk identification and analysis. To simplify the risk analysis, OCTAVE Allegro computes a relative risk score based on a quantitative measure of the threat's impact. For example, if the reputation is most important to a HEI, then to all risks impacting the HEI's reputation will be assigned a higher score. In the final step a mitigation plan has to be developed based on the computed risk score.

Another approach is the RISK IT framework by ISACA. It mandates that IT risks should always be connected to business objectives, i.e., it needs to be integrated with the overall enterprise risk management, for instance based on COSO ERM, to establish and maintain a common risk view to support the making of risk-aware business decisions. The underlying process model consists of three phases: the risk governance, risk evaluation and risk response. Risk governance, equivalent to the business and top-level management perspective, establishes the risk tolerance and risk appetite of an organization. In the risk evaluation step, the business impact of relevant risks amongst the pervasive presence of IT has to be determined using risk scenarios and various risk factors, which can be interpreted as casual factors influencing either the frequency or the business impact of a threat. Risk response requires the selection of so-called key risk indicators, which provide a forward- and backward-looking view on the organization's risk landscape, selecting an appropriate response option and its prioritization based on the associated costs, the option's effectiveness and efficiency.

Another popular risk management method is MEHARI (MEthod for Harmonized Analysis of Risk) by the Club de la Securite de l'Information Francais (CLUSIF), which was designed to align with the risk management approach of ISO/IEC 27005, i.e., its focus is on answering the *how* rather than the *why* question to do risk management. MEHARI starts by considering three types of *need* for each business activity: 1) The need of services, 2) the need of information and data required to complete the service, and 3) the need for regulatory or legal compliance. For risk identification this method differentiates between intrinsic and contextual vulnerabilities, which describe any weaknesses of a security control. Unique to MEHARI's risk management method is a knowledge base to describe risk situations. Through the mapping of implemented security services and its rated effectiveness in relation to the CIA impact of the considered risk, defining risk situations and conducting risk assessment becomes possible. CLUSIF provides Excel-based audit questionnaires to define the relevant business processes, risk management domains, the data classification, vulnerabilities. Risk situations and their impact can be derived from the questionnaires' answers and already implemented security services. Some of the questions are mapped directly to security controls described in ISO/IEC 27002, i.e., how to counteract specific threats.

The last methodology described in this section is MAGERIT. Its risk management consists of two steps, the risk analysis and the risk treatment. The analysis phase splits up into four sub-phases: the identification of primary and secondary assets, the threat identification, the determination of resulting risks, and the implemented safeguards. MAGERIT's primary assets are the processed information and provided services. Typical threats are listed in an categorized elements catalogue. A table-based assessment of the threat's impact and likelihood allows the determination of the resulting risk value. As known through the inclusion of safeguards, the risk's likelihood or its impact can be reduced. MAGERIT takes the effectiveness and maturity level of a safeguard into account, which can be a critical factor for risk assessment and determination of residual impact and risks.

Note that this overview of standards or frameworks could not be exhaustive, but gives an overview of the definition of each risk management process, its phases, and activities that have to be performed as well as of some tools, which support these tasks.

4. THE GAP BETWEEN READING ABOUT RISK MANAGEMENT AND DOING IT

On the one hand, a HEI-specific instance of the overall risk management process has to be designed and implemented, and on the other hand, this HEI-specific process needs to be practiced and prove its worth. We outline both challenges for the typical process phases in this section, and focus on a solution approach for the second challenge in the next sections.

All of the reviewed approaches define risk management as a continuous process, which usually starts with the establishment of the context. Most of the standards differentiate between primary and secondary asset types. On the one hand, higher-level management usually knows the important business processes and has a big picture of which information needs to be protected; for example, in HEIs there is an examination office and the students' personal data, such as addresses and grades, are valuable. On the other hand, the staff level, especially the technicians and system administrators, usually have in-depth knowledge about the secondary assets within their functional responsibility and sometimes also about the relationships between these assets. For example, a software-based examination management system may run on three different servers and make use of a central NAS file server for data storage. Unfortunately, none of the standards gives detailed instructions how the risk-management-relevant assets can be found adequately, i.e., neither too coarse- nor too fine-grained. As a consequence, system administrators can specify the value of hardware and software assets quite easily and make estimates of the costs related to their working time when, for example, a compromised server needs to be re-setup from scratch. But it is practically next to impossible for them to quantify the value of, e.g., one student record stored on their servers or make assumptions about the impact on the HEI reputation when the confidentiality of student records is compromised. Furthermore, all tools mentioned above require the manual definition of assets and their relationships to each other, but currently lack technical functionality to import existing data from other data stores, such as, e.g., a campus management system, an organization-wide ITIL® configuration management system, or other workflow management tools. Thus data inconsistencies are bound to occur in the long run as it is cumbersome to maintain the same data independently in different IT systems.

The next activity in the risk management process is the identification of threats affecting these assets. While ISO/IEC 27005 includes a short and quite superficial threat catalogue, the BSI IT-Grundschutz methodology provides a very comprehensive and detailed, but mostly technical view on the threat landscape. The others favor the description of threat or risk scenarios, but usually do not give some details in form of a template or table to perform this step. One typical problem is the definition of risk categories and which groups of people should consider them in which depth. For example, damage to assets caused by earthquakes, fire, or floods do not need to be dealt with by each system administrator separately when a common room for all servers is used; on the other hand, the service-specific risks may vary greatly between web-based applications, so it may not be wise to treat all web-based applications equally during risk identification.

For risk analysis and risk assessment, the frameworks differentiate between quantitative, qualitative, and semi-qualitative (NIST 800-30) approaches. Usually there are example tables to describe the method by itself, but each organization has to find its own best-fitting approach. The risk assessment has to take existing safeguards into account, but only MAGERIT's approach assesses their effectiveness and maturity. The other approaches pursue an all-or-nothing risk treatment. Quantitative risk assessment is non-trivial, especially when already the value of an asset is hard to quantify, as is the case with many information assets, such as a student record or the HEI president's email account. Also the likelihood of a risk can often only be roughly estimated. A simplified approach is consider how often a risk materialized in the past to make an educated guess about how often it will occur in the next timeframe; this, however, does not take into account changes to the threat landscape – for example, a zero-day exploit may compromise a server that never had any security incidents before.

For the risk treatment phase, the standards ISO/IEC 27001, appendix A and the corresponding code of practice document provide some means to reduce the likelihood of risk materialization or its impact. These standards lack a direct mapping of threats, resulting risks to a list of suitable security controls to act upon these risks as it can be seen in BSI IT-Grundschutz methodology or partly in CLUSIF's MEHARI. Matters are complicated further by the fact that the top management's and technical staff's point of views usually do not match in the risk treatment. While the former often prefer to define policies and processes, the latter want to implement technical countermeasures.

Therefore, a typical state of projects implementing risk management at HEIs is that process specifications inspired by standards and good practice frameworks are written and the processes officially come into operation, but comprehensive implementation cannot be achieved because the involved stakeholders do not comprehend what and how exactly they should contribute and how

they could benefit from the results. Enabling the more technically focused staff to contribute to and benefit from a HEI-wide risk management is the goal of our approach presented in the next section.

5. OPERATIONALIZING THE RISK MANAGEMENT PROCESS

In this section we provide a template-based risk management approach primarily intended for responsible system and service administrators. In our security concept documentation template, which we presented at EUNIS 2013, the administrators have to describe, among many other security-relevant parameters, the risks specific to their services. When filling out this template, often the following questions arose:

- How can I identify all the assets implementing or supporting the described service?
- How can I determine an asset's criticality and value?
- How can specific threats be identified? Are there any catalogues available, maybe specific for, e.g., a Linux-based server, webserver, or a database server which can be used as a starting point?
- What information is required for describing a threat? Is a very fine-grained scenario description necessary or are some keywords sufficient?
- Which metrics or classification scheme can be used to determine the likelihood and impact of risks?
- How can I formulate already implemented safeguards? How do I have to describe the already planned measures that will be implemented to reduce or avoid an identified risk?
- How do I have to document the risk identification and analysis? How often do I have to repeat these activities?

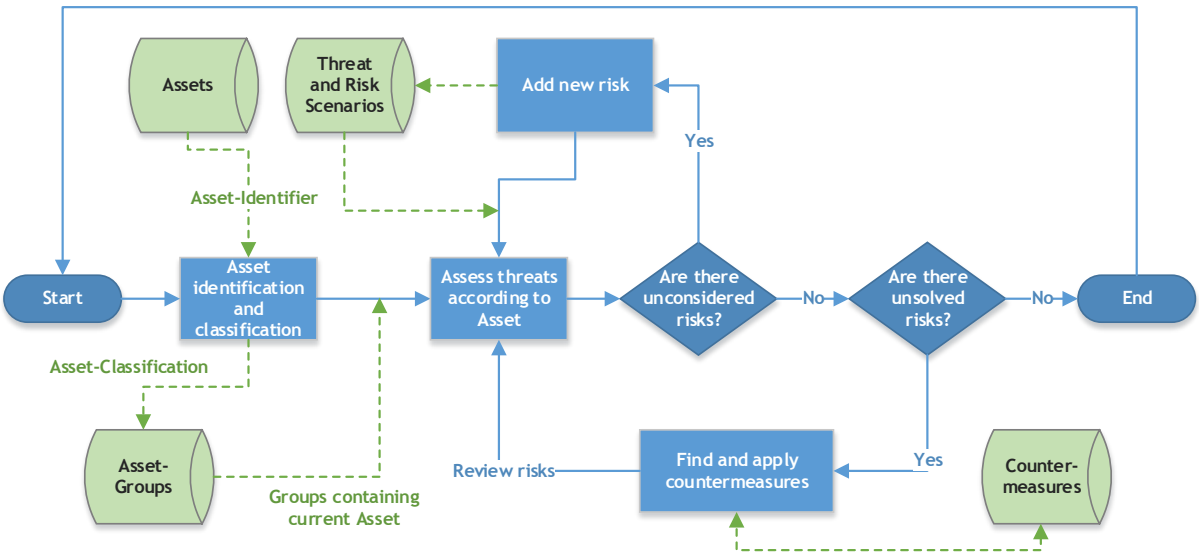


Figure 1: Workflow overview – integrating a new asset

An important aspect that will improve the willingness to contribute to a risk management process is enabling as much flexibility as possible. Thus, the approach provides reusability of most parts of the institution's already existing management infrastructure:

One essential element, most HEI's already implemented, a Configuration Management Database (CMDB), serves as one data source for describing details about secondary assets. Other data sources, providing similar information can also be connected using defined interfaces, e.g., import of csv-files or direct access to databases. Operating such a CMDB is one important step on the way leading to a successful risk management, because it usually contains numerous information required for asset identification and provides all functions to add, change, and remove them.

The following step - denoted as asset classification - can be done separately with references to the particular asset in the CMDB.

Figure 1 shows an exemplary integration of several data sources interdepending on the overall risk management process. The states (shown in blue) describe the several steps to integrate an asset, whereas the green glyphs and the dashed lines describe required data sources, information, and interaction with the user.

The implementation possibly benefits from a decoupled structure of data sources, since it can be done without affecting the existing infrastructure. Therefore, on the other hand, there is a need to associate them with each other, which can be achieved by an unique item identification and references among the data sources. As the overall approach of providing a structured template as guidance for writing security concepts was well received, a similar approach was taken to foster information security risk management on the system administrator level. It covers the aspects described in the following sections.

5.1. Asset identification, grouping, and criticality

System and service administrators focus on technical aspects implementing and supporting the provided services. Thus the business perspective or any associated strategic objectives that have to be achieved are mostly out-of-scope of their risk management activities. Natural risks, such as floods and earthquakes, as well as threats targeting the data center's buildings and specific security areas or rooms usually have a very huge negative impact on all services provided by the HEI. But because of their comprehensive characteristics, such risks have to be taken into account in the risk management procedure by the facility management staff and not by each individual administrator.

The administrator's focus is on technical assets - which generally serve as basis for the HEI's services, so each asset usually belongs to one of the following groups:

- **Communication Infrastructure**, at which, on a more fine-granular level, those assets can be a part of the network connection cabling or network components like routers and switches.
- **Device Infrastructure**, split at least into physical and virtual hosts.
- **Software**: As soon as an administrator deploys a new host, this is probably the most comprehensive asset class to consider. The huge diversity of software makes it practically impossible to register all risks; then again, it is even more important to reduce the risk to a HEI's acceptable level. Thus, the consideration of operating systems (Microsoft Windows, Linux, BSD, …), service software (e.g., web services, database services, …), further associated applications like runtime-environments (e.g., JRE, Perl, …) and self-made software will provide a lot of benefits.
- The **Service** context and related **Information**. Obviously, important aspects are login credentials as well as user accounts and the data being processed within the service. For instance, PII requires - mostly due to statutory and regulatory requirements - higher protection levels than publicly available or only slightly critical information. Also, essential configuration files can be seen as critical assets, since they are one with the highest relevance for information security.

Grouping of the identified assets simplifies the risk management process by reducing the complexity of asset-threat relations because threat scenarios descriptions can be reused assets with similar specifications; it also is a simple approach to support the provisioning of user-friendly views of the data with additional functionalities like filtering and risk preselection.

To determine the asset's criticality, the administrator has to answer the following, exemplary questions depending on the asset type and confidentiality, integrity, and availability requirements:

- How many users are affected if the service is not available or partly not available due to a hardware defect, software configuration failure, or when taken offline due to a security incident? Typical answers for a HEI's environment and if a service explicitly provided for students will be affected are either less or more than 1.000 users.
- What impact does an accidental or deliberate disclosure of critical information have, e.g., from a legal point of view, for the HEI's reputation, for each user, and so on, broken down

into some simplified related questions like “Does the service or any component process or store PII data, e.g. name, email address, account data, IP addresses? If so then this can be directly mapped to applicable data protection laws and eventuate in a high asset value.

- Can assets be effectively grouped to assign a value to the group rather than to each asset itself, e.g., workstations of HEI employees? But do any differences between such group members exist, based on, e.g., their specific role and duties within an organization? Typical, simplified questions to answer can be, e.g. “Does your role in the organization demands direct or indirect access to PII data?” or “Does your role in the organization imply administrative access to more than 25 server machines, e.g., as an administrator responsible for the virtual server environment?”

5.2. Threat identification and description

Based on the identified assets and asset types, the administrators have to identify and describe threats. Based on threat catalogues provided by ISO/IEC 27005 and BSI IT-Grundschutz threat and risk scenario templates are used containing the following information:

- **Actor**: The trigger or cause of a threat or damage occurring. This can be for instance an external adversary, an employee of a contractor, an insider or even a guest, who uses the service temporarily, or any other event that takes place threating the e.g., the availability of the whole service or integrity of the processed information.
- **Threat type**: Allow the categorization of threats, e.g., malicious intent, accident or error, failure of hardware or software component used, or external requirements based on statutory or compliance frameworks.
- **Event**: Short description of the threat event itself, also based on a category like disclosure of critical information, service interruption, unauthorized modification of critical information resulting in erroneous results, theft, destruction, ineffective service provisioning, violation of existing policies, rules and regulations at a higher level or inappropriate usage of a service or supporting component.
- **Asset**: The threat’s description should contain information about the affected assets, e.g., the service infrastructure, the information or application.
- **Time**: This element can be used to describe further details about the threat’s duration, the time the threat event occurs, or the time needed to detect security-related events.

The question the HEI’s risk manager has to ask at this point is “How many risk or threat scenarios can be managed?”. One technique of keeping the number of scenarios manageable is to develop a set of more generic scenarios throughout the HEI, but also apply more detailed scenarios in which risk levels are assumed to be significantly higher. The following example describes a high-level risk scenario to describe threats affecting a database’s integrity:

- Actor: internal and external
- Threat type: failure, malicious
- Event: intentional modification failed, data corruption (unauthorized client’s transactions)
- Asset: database used by described service
- Time: duration (unknown), timing (unknown)

5.3. Risk assessment

In the next process step the identified threats have to be analyzed and assessed. The analysis is usually easier to perform when following a qualitative instead of a quantitative approach. For the determination of the risk likelihood, the following questions are relevant and have to be answered by the service administrators:

- How do you categorize the accessibility of your service and how many users typically use the service? The likelihood of a risk materializing is obviously higher, if a huge number of users has access to the provided service. The accessibility should also be taken into account because those services, which have to be provided for users outside the HEI’s internal

communications network, may eventually be compromised by any private, not controllable client machine via the Internet. In both cases the likelihood often has to be assumed high.

- Do any known vulnerabilities exist in the service or one of the underlying components and cannot be fixed for given reasons? Some services require certain software versions. Updating the software can have either incalculable side-effects or interfere, for instance, with the stability of the service or additionally require an update on the client-side and may therefore not be acceptable. If such vulnerabilities exist and, e.g., can be exploited over the Internet even by inexperienced attackers, then the likelihood should be set to a high value.
- Has the service or any underlying component already been part of a security incident that occurred in the past? If so, did you take any additional countermeasures that prevent similar incidents from occurring again? The likelihood that a perpetrator will return if a service has already been part of a security incident may be high because the IP address of the server machine may have been published in an underground community, because a backdoor installed by the first successful compromise may not have been removed completely or the measures taken are not as effective as planned.

On the other hand, service administrators have to determine the impact of an occurring threat event. Based on the already described criticality estimation of the asset concerned, a direct qualitatively mapping to the threat's impact is often possible. A short example:

- Number of affected users: If less then 10 users are affected, then the risk has a low impact. If, however, even more than 1.000 users are affected, then the impact is very high.
- Any legal regulations can be concerned: If yes, then the impact should also be very high.

If for each threat and asset the impact mapping has been performed, this can result in different impact levels. For example, a threat or resulting risk can have a very high impact on the affected users but no regulatory impact (e.g., not concerned = low); then, the highest impact value has to be assigned to this risk.

For risk assessment usually both, the likelihood and impact values have to be combined. An event with a medium likelihood and a very low impact usually does not require further treatment action. But, on the other hand, threat events with a low likelihood but a very high impact should be taken into consideration, because even a single occurring event would affect a huge number of users or the HEI as a whole.

5.4. Risk treatment

After finishing the risk assessment, the risk management approaches discussed before usually provide four treatment options (reduce, avoid, accept, or transfer). From a technicians perspective only two, reducing the risk by appropriate countermeasures and risk avoidance through the removal or replacement of vulnerable components are feasible. Because risk avoidance often requires major changes to the service provisioning itself or also the procurement of new hardware and software, this section concentrates on countermeasures with a view to reduce the risk..

Each countermeasure has to be specified, planned, documented and maybe linked to a request for change from the IT service and change management point of view.

For the specification of a countermeasure, also the usage of a template-based approach is recommended containing the following mandatory and optional information, which enables the instantiation of a specific risk treatment option:

- **Unique ID**: A countermeasure (template) must be clearly recognizable for referencing purposes.
- Short **description** of the countermeasure.
- **Responsible for implementation**: The person responsible that overviews and monitors the implementation of the countermeasure.
- **Completed until**: The implementation should be completed until the defined point of time.
- **Tasks**: Description of each task to implement the countermeasure, maybe linked to a request for change in the context of the change management procedure of the HEI.

- **Implementation requirements**: Usually IDs of other template instances describing countermeasures that have to be completed before or have also to be completed in parallel to or following this implementation.

Through instantiating a specific template to reduce the likelihood or impact of a certain risk the risk's treatment can be described. From a business people perspective the goal is to achieve at least an acceptable remaining risk level. From a service administrator's point of view only the implementation of the suggested countermeasures has to be done. Afterwards the risk analysis has to be repeated until all not acceptable risks are taken into account and appropriate countermeasures have been implemented and documented.

6. BEYOND BORDERS: INTER-ORGANIZATIONAL RISK MANAGEMENT

Nowadays HEI's services are not only provided for their own employees or students, but rather eLearning, high-performance computing, grid and cloud-based services, e.g. sync-and-share file storage services are provided inter-organizationally. Because the security of these services remains as one complying requirement, information security management and especially risk management also have to be performed across HEIs' borders. For instance, if one HEI centrally provides a sync-and-share file service for all or some institutions of the European research community, this is, from a technical security and especially a risk management perspective, comparable to an outsourced service in the private enterprises sector. The service consumer, e.g., also a HEI, therefore remains responsible for information processed by the outsourced service, but can not directly act upon the cloud-service provider's infrastructure, security, and risk management processes.

For example, the identification of assets must take place in a distributed fashion. On the one hand the customer HEI and on the other hand the service provider HEI have to identify the service-related assets. The provider contributes information about the used server hardware, the network components, and the software installed. From the customer's point-of-view, the transferred and on the provider's side stored or otherwise processed information are critical and protection-worth assets. To determine the asset's value, the provider's administrators usually use their own organization-internal scheme as discussed in the previous sections. The customer or even each service user have to determine the information's value using another criticality scheme because only they have the required knowledge about the sensitivity and classification of their data. The identification of threats also varies when compared to intra-organizational risk management. Threat catalogues used by one HEI may differ from those used within the others. Analogously, the procedures to derive the results of the likelihood and the impact estimation of a threat event materializing are often different. For example, if the service customer uses a scheme to qualitatively determine the likelihood of a risk related to the information assets, which consists of four levels (low, medium, high, very high), but the provider uses five likelihood levels (very low, low, medium, high, very high), then a direct mapping of these different schemes is required or a new scheme to be commonly used in the cooperation must be designed.

7. CONCLUSION

Risk management is the key to successful information security management. In turn, risk management can only be successful if a risk management process is not only specified on paper, but also practiced. Unfortunately, standards and good practice frameworks can only provide generic guidance and each HEI must find its own way to put this knowledge into real-world practice. The major problem addressed in this article is how to get the technology-oriented members of the staff level practically involved in HEI-wide risk management, which is often perceived as abstract, bureaucratic, and without practical benefit on the technical level. We presented a checklist-style approach and exemplary questions that helps system administrators with the individual risk management steps asset and criticality identification, threats identification and description, risk assessment, and risk treatment. It complements the security concept documentation template presented at EUNIS 2013. Finally, an outlook to inter-organizational risk management, e.g., as part of HEI cooperation and research projects, was given. The long-term goal of our activities is to compile the feedback we receive into a HEI best practice guide on information security risk management, so any suggestions for improvement are highly welcome.

8. REFERENCES

[1] Wolfgang Hommel, Stefan Metzger, Helmut Reiser, and Felix von Eye (2013), IT security concept documentation in higher education data centers: A template-based approach, in: ICT Role for Next Generation Universities, 73–83, RTU Press, Riga, Latvia, June, 2013.

[2] ISO/IEC 27005:2011, Information technology — Security techniques — Information security risk management, Genoveva, Switzerland, 2011

[3] BSI IT-Grundschutz Catalogues: 13th version, Bonn, Germany, 2013, https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz.html

[4] NIST Special Publication 800-30rev1, Guide for Conducting Risk Assessments, Recommendations of the National Institute of Standards and Technology, Gaithersburg, September, 2012

[5] NIST Special Publication 800-39, Managing Information Security Risk - Organization, Mission and Information System View, Recommendations of the National Institute of Standards and Technology, Gaithersburg, March, 2011

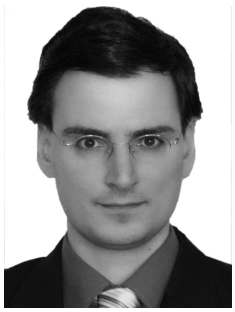
[6] Introducing OCTAVE Allgegro: Improving the Information Security Risk Assessment Process, Carnegie Mellon University, May, 2007

[7] ISACA, The Risk IT Framework, 2009, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx

[8] MEHARI, Information risk analysis and management methodology, Club de la Sécurité de l'Information Français (CLUSIF), Paris, 2010, https://www.clusif.asso.fr/en/production/mehari/

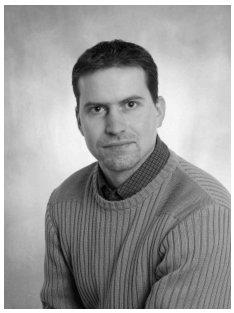
[9] MAGERIT V2.0, Methodology for Information Systems Risk Analysis and Management, Ministerio de Administraciones Publicas, Madrid, 2005, http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en#.VN4Ehsap3dk

9. AUTHORS' BIOGRAPHIES



Wolfgang Hommel is the Chief Information Security Officer of the Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities, where he is also the head of the communication networks planning group.

He studied computer science at Technische Universität München and has a Ph.D. as well as a postdoctoral lecture qualification from Ludwig-Maximilians-Universität in Munich, Germany, where he teaches information security lectures and labs. His research, for which he was granted the Karl Thiemig foundation's young academics award in 2011, focuses on information security and IT service management in large-scale and inter-organizational scenarios.



Stefan Metzger is member of the communication networks planning group at the Leibniz Supercomputing Centre. He holds an international CISSP certification. As head of the LRZ security working group his main focus lays on ISO/IEC 27000-based security management.

He attained in 2005 a Diploma degree in Computer Science from Technical University Munich. Currently he's doing his PhD in security management in large-scaled, inter-organizational infrastructures and offers lab courses in security at Ludwig Maximilians University (LMU) Munich.

Michael Steinke is currently completing his master's degree in computer science at the Ludwig-Maximilians-University in Munich, where he acquired his bachelor's degree in 2013 as well. He works as a research assistent in the security working group at Leibniz Supercomputing Centre and his current research activities focus on information security, vulnerability, and risk management.