# A Method for Re-using Existing ITIL Processes for Creating an ISO 27001 ISMS Process Applied to a High Availability Video Conferencing Cloud Scenario

Kristian Beckers, Stefan Hofbauer, Gerald Quirchmayr, Christopher C. Wills

# A Method for Re-Using existing ITIL processes for creating an ISO 27001 ISMS process applied to a high availability video conferencing cloud scenario

Kristian Beckers[1], Stefan Hofbauer[2],
Gerald Quirchmayr[3,4], and Christopher C. Wills[5]

[1] University of Duisburg-Essen, paluno - The Ruhr Institute for Software Technology
Kristian.Beckers@paluno.uni-due.de
[2] Amadeus Data Processing GmbH, Network Integration Services
Stefan.Hofbauer@amadeus.com
[3] University of Vienna, Multimedia Information Systems Research Group
gerald.quirchmayr@univie.ac.at
[4] University of South Australia, School of Computer and Information Security
gerald.quirchmayr@unisa.edu.au
[5] CARIS Research Ltd.
ccwills@carisresearch.co.uk

**Abstract.** Many companies have already adopted their business processes to be in accordance with defined and organized standards. Two standards that are sought after by companies are IT Infrastructure Library (ITIL) and ISO 27001. Often companies start certifying their business processes with ITIL and continue with ISO 27001. For small and medium-sized businesses, it is difficult to prepare and maintain the ISO 27001 certification. The IT departments of these companies often do not have the time to fully observere standards as part of their daily routine. ITIL and ISO 27001 perfectly fit into companies and help reduce errors through the standardization and comparability of products and services between themselves and other companies and partners. ISO 27001 specifically looks at security risks, countermeasures and remedial actions.

We start with the processes that need to be in place for implementing ITIL in an organisation's business processes. We use a cloud service provider as a running example and compare ITIL processes with ISO 27001 processes. We identify which aspects of these two standards can be better executed. We propose a mapping between ITIL and ISO 27001 that makes them easier to understand and assists with the certification process. We show further how to prepare for audits as well as re-certification. Often, these two processes are seen separately and not in conjunction, where synergies can be exploited. Legal requirements, compliance and data security play an integral part in this process. In essence, we present checklists and guidelines for companies who want to prepare for standardization or that are already certified, but want to improve their business processes. We illustrate our method using an high availability video conferencing cloud example.

**Key words:** ITIL, ISO 27001, cloud computing, processes, standards, certification, compliance

# 1 Introduction

Before an organisation can consider becoming certified and begin applying certified standards, there must be a clarity of understanding in relation to the organisation's business processes. These processes must be defined, agreed and adopted. The organisation must understand, the service level agreements (SLA) operated by their clients or customers and which services the organisation offers as managed service provider. For audit reasons this knowledge must be reviewed twice a year and any emergent changes need to be documented.

Another important step is the introduction of a ticketing system, like open source product OTRS, to capture all customer interactions and support the processes. The ticketing system should also contain an asset inventory, where all hardware and software is itemised. Every update, addition, change or deletion must be reflected in this inventory. Additionally hardware and defined services should be monitored, perhaps with an open source software such as Nagios [6] for example.

The move towards cloud services is accelerating the rate at which companies develop and the use of such service requires the sharing of large amounts of data in a secure and scalable way. ITIL and ISO 27001 help companies to achieve customer friendliness and high quality services and support. Without standardization, a lot of manual effort, growing cost and complexity for an organization arises, as the number of their service partners grows.

An organisation should definitely start with certifying ITIL and proceed with the ISO 27001 aiming at security afterwards. The basis for the ITIL certification is an understanding of ITIL itself, quality assurance and knowledge of the business processes in place. Capacity management assures that there is no capacity shortage on the provider side, as well as on the customer side. Regular checks and warnings, based on defined thresholds help to meet the capacity requirements and plan for expected growth. Exceptionally fast growth or the adding of resources must be planned, organized and scheduled, with the cloud provider service manager. This is an important step towards supporting the client or customer. At the base of the organisational hierarchy is the first level desk, then the technical engineers, the service manager and a department manager or even chief executive officer. The involvement of these roles depends on the defined SLAs and the target-, reaction time to solve incidents.

The rest of the paper is organized as follows. Section 2 presents background on the standards ITIL and ISO 27001. Section 3 serves as structured method for Section 4, which shows how these two standards can be mapped and mutual benefit created from the synergy between each other. Section 5 shows a usage example of the method based upon a real-life example and Sect. 6 presents related work. Section 7 concludes and gives directions for future research.

[6] http://www.nagios.org

## 2 Background

We illustrate the general idea of cloud computing in Sect.2.1, and our cloud system analysis pattern in Sect. 2.2. We introduce the ISO 27001 standard in Sect. 2.3 and the ITIL Standard in Sect. 2.4.

### 2.1 Cloud Computing

The term *cloud computing* describes a technology as well as a business model [1]. According to the *National Institute of Standards and Technology (NIST)* cloud computing systems can be defined by the following properties [2]: the cloud customer can acquire resources of the cloud provider over *broad network access* and *on-demand* and pays only for the used capabilities. Resources, i.e., storage, processing, memory, network bandwidth, and virtual machines, are combined into a so-called *pool*. Thus, the resources can be virtually and dynamically assigned and reassigned to adjust the customers' variable load and to optimize the resource utilization for the provider.

The virtualization causes a location independence: the customers generally have no control or knowledge of the exact location of the provided resources. Another benefit is that the resources can be quickly scaled up and down for customers and appear to be unlimited, (this is called *rapid elasticity*). The pay-per-use model includes guarantees such as availability or security for resources via customized *Service Level Agreements (SLA)* [3].

The architecture of a cloud computing system consists of different service layers and allows different business models: on the layer closest to the physical resources, the *Infrastructure as a Service (IaaS)* provides pure resources, for example virtual machines, where customers can deploy arbitrary software including an operating system. Data storage interfaces provide the ability to access distributed databases on remote locations in the cloud. On the *Platform as a Service (PaaS)* layer, customers use an API to deploy their own applications using programming languages and tools supported by the provider. On the *Software as a Service (SaaS)* layer, customers use applications offered by the cloud provider that are running on the cloud infrastructure. Furthermore, cloud providers require a layer that monitors their customers' resource usage, e.g. for billing purposes and service assurances. Buyya et al. [4] introduce this layer as a middleware in their cloud model. Cloud computing offers different *deployment scenarios*: *private clouds* are operated solely for an organization, *public clouds* are made available to the general public or a large industry group and are owned by a third party selling cloud services. In between these scenarios are *hybrid clouds* where users complement internal IT resources upon demand with resources from an external vendor [1].

### 2.2 Cloud System Analysis Pattern

We propose patterns for a structured domain knowledge elicitation. Depending on the kind of domain knowledge that we have to elicit for a particular software engineering process, we always have certain elements that require consideration. For this work we use a specific *context elicitation pattern*, the so-called *cloud system analysis pattern* [5]. We base our approach on Jackson's work on Problem Frames [6] that considers

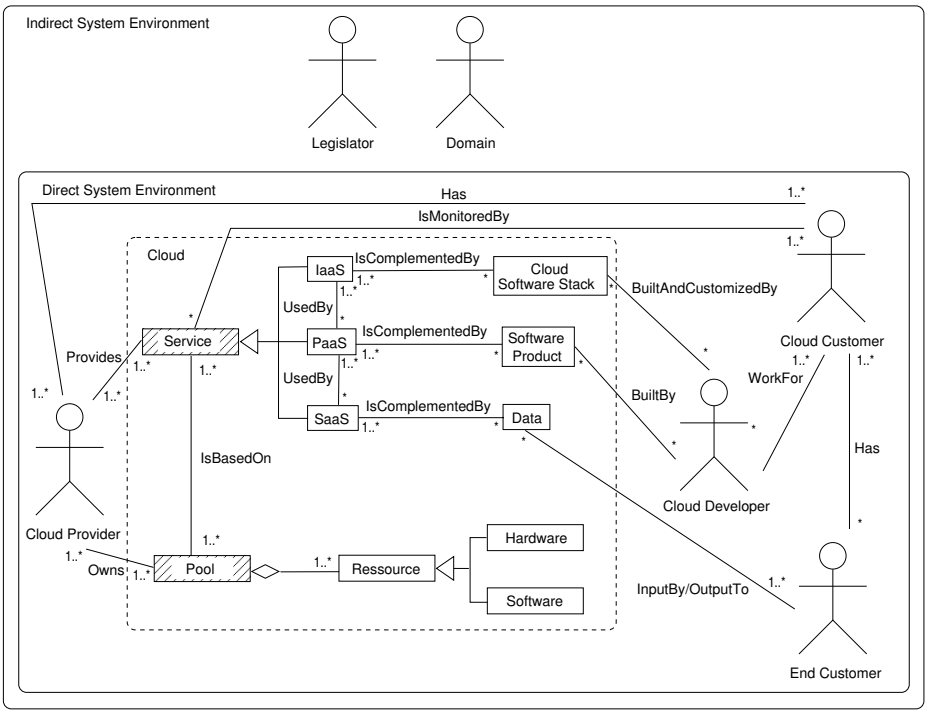


**Fig. 1.** Cloud System Analysis Pattern taken from [5]

requirements engineering from the point of view of a machine in its environment. The machine is the software to be built and requirements are the effect the machine is supposed to have on the environment. Any given environment considers certain elements, e.g., stakeholders or technical elements. Jackson [6], who describes Problem Frames as follows: *"A problem frame is a kind of pattern. It defines an intuitively identifiable problem class in terms of its context and the characteristics of its domains, interfaces and requirement."*. We were also informed by Fowler [7]. Fowler, developed patterns for the analysis phase of a given software engineering process. His patterns describe organizational structures and processes, e.g., accounting, planning, and trading.

Our patterns for the analysis phase differ from patterns concerning solutions for the design phase of software engineering like the Gang of Four patterns [8] or the security patterns by Schumacher et al. [9]. The reason is that we provide a means for a structured elicitation of domain knowledge for cloud computing systems. We do not provide solutions for the implementation phase of clouds. We present a short introduction of our so-called *Cloud System Analysis Pattern (or short: Cloud Pattern)* [5] in the following. We created the pattern for cloud-specific context establishment and asset identification compliant to the ISO 27000 series of standards. A *Cloud* (see Fig. 1) is embedded into an environment consisting of two parts, namely the *Direct System Environment* and the *Indirect System Environment*. The *Direct System Environment* contains stakeholders and other systems that directly interact with the *Cloud*, i.e. they are con-

nected to the cloud by associations. Moreover, associations between stakeholders in the *Direct* and *Indirect System Environment* exist, but not between stakeholders in the *Indirect System Environment* and the *Cloud*. Typically, the *Indirect System Environment* is a significant source for compliance requirements. The *Cloud Provider* owns a *Pool* consisting of *Resources*, which are divided into *Hardware* and *Software* resources. The provider offers its resources as *Services*, i.e. *IaaS*, *PaaS*, or *SaaS*. The boxes *Pool* and *Service* in Fig. 1 are hatched, because it is not necessary to instantiate them. Instead, the specialized cloud services such as *IaaS*, *PaaS*, and *SaaS* and specialized *Resources* are instantiated. The *Cloud Developer* represents a software developer assigned by the *Cloud Customer*. The developer prepares and maintains an *IaaS* or *PaaS* offer. The *IaaS* offer is a virtualized hardware, in some cases it is equipped with a basic operating system. The *Cloud Developer* deploys a set of software named *Cloud Software Stack* (e.g. web servers, applications, databases) into the *IaaS* in order to offer the functionality required to build a *PaaS*. In our pattern *PaaS* consists of an *IaaS*, a *Cloud Software Stack* and a *cloud programming interface (CPI)*, which we subsume as *Software Product*. The *Cloud Customer* hires a *Cloud Developer* to prepare and create *SaaS* offers based on the CPI, finally used by the *End Customers*. *SaaS* processes and stores *Data* input and output from the *End Customers*. The *Cloud Provider*, *Cloud Customer*, *Cloud Developer*, and *End Customer* are part of the *Direct System Environment*. Hence, we categorize them as *direct stakeholders*. The *Legislator* and the *Domain* (and possibly other stakeholders) are part of the *Indirect System Environment*. Therefore, we categorize them as *indirect stakeholders*. We also provide templates for each stakeholder that describe their attributes like motivation for using the cloud.

### 2.3 The ISO 27001 Standard

The ISO 27001 defines the requirements for establishing and maintaining an Information Security Management System (ISMS) [10]. In particular, the standard describes the process of creating a model of the entire business risks of a given organization and specific requirements for the implementation of security controls. The ISO 27001 standard is structured according to the "Plan-Do-Check-Act" (PDCA) model, the so-called *ISO 27001 process* [10]. In the *Plan* phase an ISMS is established, in the *Do* phase the ISMS is implemented and operated, in the *Check* phase the ISMS is monitored and reviewed, and in the *Act* phase the ISMS is maintained and improved. In the *Plan* phase, the *scope and boundaries* of the ISMS, its *interested parties*, *environment*, *assets*, and all the *technology* involved are defined. In this phase also the ISMS *policies*, *risk assessments*, *evaluations*, and *controls* are defined. Controls in the ISO 27001 are measures to *modify risk*. The ISO 27001 standard demands the creation of a set of documents and the certification of an ISO 27001 compliant ISMS is based upon these documents.

Changes in the organisation or technology also have to comply with the documented ISMS requirements. Furthermore, the standard demands periodic audits towards the effectiveness of an ISMS. These audits are also conducted using documented ISMS requirements. In addition, the ISO 27001 standard demands that management decisions, providing support for establishing and maintaining an ISMS, are documented as well. This support has to be documented via management decisions. This has to be proven

as part of a detailed documentation of how each decision was reached and how many resources are committed to implement this decision.

### 2.4 The ITIL Standard

The IT Infrastructure Library (ITIL) [11] is a collection of best practices for implementing an IT service management. The standard provides example processes for typical tasks regarding IT management. The standard also provides tools of how to consider planning, establishing, supporting and optimizing of IT services in order to achieve business goals.

ITIL is a defacto standard for the creation, establishment and management of critical processes. ITIL contains generic descriptions and is independent of vendors or technology. ITIL provides a set of process that contain: basic requirements for the process, goals of the process, pattern for procedures and roles, interfaces for different processes, hints for critical success factors, suggestions for measuring key performance indicators, knowledge about success criteria for deploying the process.

## 3 Method

Cost, flexibility and ease of operation are driving more and more organisations into the cloud. We differentiate here between the public cloud, with cloud services of providers such as Amazon or Salesforce and the private cloud of virtualised services running on an organisation's privately run hardware and software.

It is not easy for a huge organisation to transition everything over to the cloud at once, because then parts of the business critical systems and services are already transitioned into the cloud and some are not. Cloud integration platform help solve this issue and help unite those services.

With the cloud integration platform it becomes much easier for global cloud players to sell cloud services to their partners. We consider clouds in our method via using our cloud system analysis pattern introduced in Sect. 2.2.

### 3.1 ITIL

Our practical experience has been, gained in different organisations, both mid-sized to large. From this experience, we identify the following steps relevant for implementing ITIL within a company. Different roles must be introduced and are needed to comply with this standard.

**Define initial Tasks for the Roles** Our method requires a service manager, who is having regular service meetings with the service provider, as well as a service desk including a service manager. The service desk covers agreed service times and may also be on duty after business hours for special reasons, such as emergency incidents. A change advisory board is established, whose task is to supervise proposed changes and confirm or cancel those changes. Changes can be cancelled for instance if no fallback is available, or the risks are too high. Field engineers work

closely together with external customers to help fulfil their business needs. They are part of the service desk, but most of the time, are not at the office. The service manager, together with the service desk manager is also responsible that the customer gets a SLA report at least once a month. If the SLA criteria are not met, the service provider must reimburse as defined in the service contract between these two parties.

**Create an Incident Response System** The service desk uses a ticket system, such as OTRS for incident management, as well as capacity management and inventory management. The ticketing system also keeps track of the guaranteed reaction time and time to recover for incidents. Service engineers can use the ticketing system to record their invested support time, which can then be used for billing purposes, as well as a means to communicate with the customer through e-mails. The agreed SLA values are part of the service contract and can be further negotiated by both sides, assuming the mutual consent.

**Establish a Monitoring System** It is the duty of the service provider to monitor their own core infrastructure as well as customer devices. If requested, the service provider can also monitor devices within the customer site. The monitoring solution automatically generates tickets, based on the occurrence of incidents. The certified service provider needs a thorough documentation of their main business processes and service processes, including revisions on a regular basis. Every change in a productive environment, whether within the service provider context or the customer side, must be documented in a change document. Escalation processes need to be in place for incidents or problems. It must be clear, when a ticket is escalated and to whom.

**Getting certified in the core business areas** It is obviously a good idea to have trained and certified personal, because it will reduce the chance of errors as well as having a better relationship to third level partners and a better reputation against customers. For the non-daily business, a project manager is supervising the project's tasks and can acquire additional resources or take other necessary decisions. To have a clear vision of the provided services the service provider should have a service catalog for the provided service, with responsibilities and boundaries to partners. This information must be agreed on and communicated, prior having a contract with a customer. Not only the software or hardware producer is acting as third level support, but also external consultants or other companies, partners for third level support. Additional feature requests in upcoming software releases can be wished for at software partners.

**Document all necessary information** The provided service needs to be documented for technical as well as organizational aspects and revised, whenever there is a change. This documentation should be stored on a document management system, like Sharepoint, where it is easy to check out documents, make changes and check in the new document. For every customer, there needs to be a technical as well as sales person. The most important customer satisfaction parameters are availability, costs, service, innovation, upselling products as well as security. The security is of high importance for the provider's as well as customer's equipment. This includes the regular patching of devices and yearly external security audits.

**Define boundaries to stakeholders** The customer further needs a system specification and operating procedures handbook. For customer projects a project plan, time plan and dedicated project manager is needed from service provider side. The service provider should also think about a certified quality assurance employee, who takes care after quality management and quality assurance. This person needs to communicate a lot with externals as well as all involved internal departments. If the quality of the service is not assured, it is most likely that the customer will not continue the contract or as a worst case, cancel the contract with the service provider immediately. A service provider should have a service catalog, where all provided services and the engineers' responsibilities are listed.

### 3.2 ISO 27001

Once an organisation has been successfully certified in the area of ITIL, it is time to seek compliance with ISO 27001. As with ITIL, the introduction of the standard within the oranisation is made up of different sub steps.

**Agree on an IT security policy** In order to become certified in the field of ISO 27001 an organisation has to adopt the following steps. The first requirement is that of a company security policy, which handles topics, such as choosing a secure password, rights of usage of the Internet and corporate e-mail, locking of the computer, data leakage and prevention, social engineering, storage of data and confidence regarding data and information. Regular awareness training for users and administrators is provided by instructors, in order to familiarize key personal with the security policy. After the security policy training, the attendees should give their written consent, in order that the security policy can be instituted.

**Establish the position of a CISO** Furthermore, the position of a Chief Information Security Officer (CISO) is required. This position can be led by a person, who is also responsible for other topics within the company. The tasks of a CISO includes policies, standards, procedures, architecture and guidelines for the organisation's business. The first priority is the establishment of an information security function to ensure that all the organisation's information assets are well protected and mitigations are adequately implemented. The CISO will also manage the ongoing execution of the security operation in all of the organisation's information technology areas such as applications, data protection, data communications systems as well as all information systems.

Other tasks carried out by the CISO drive the overall direction of the information, application and operational security architecture as well as creating an understanding of risks by analysing and forecasting threats to information security. Moreover, the CISCO role includes managing security monitoring, analysis, detection and going through incident response processes fostering information security awareness and promoting a culture of information security and privacy.

**Document all changes** A change log document helps in keeping track of every change on productive systems for traceability and clearness. The service provider needs physical and IT security in place to defend the data centre from intruders. Therefore centre personnel need to be trained regularly. Part of these controls, are access

control of the data centre and video surveillance of the server rooms. It must be clear, who has had access to which server rack at which time. Normally, video recording tapes are digitally stored for 24 hours and when there is no reported incident, they are erased.

**Plan on business continuity and disaster recovery** The service provider's data centre needs physical and logical redundancy for all IT equipment (software and hardware) as well as a disaster recovery and business continuity plan for the data centre. The service provider should formulare a disaster recovery plan together with partners, at least once a year. A thorough documentation of all relevant security processes builds the basis for an ISMS that supports the execution of the security policy.

**Ensuring effective risk management** Identify the information assets within the company that need to be protected and conduct an accurate risk assessment on them. With risk management, the risk can be handled or even accepted, when the costs for preventive measurements are too high. Before conducting a risk assessment it is well known to first classify the information assets based on their relevance and company impact. The assessor must know if their Confidentiality, Integrity or Availability can be compromised and to which extent.

**Produce a control list consisting of action items** The controls are made up of the risk assessment again and the overall approach for mitigating or leaving risks. Selected controls should be mapped to Annex A of the standard, which consists of 133 controls in 11 domains. A review of Annex A is used to figure out, if any control areas have been missed out in the compliance process.

## 4 A Mapping between ITIL and ISO 27001 action items

The two standards, ITIL and ISO 27001 are capable of mappings between them. We are using steps from the ITIL process as input for the ISO 27001 process. With these inputs, an output can be generated. Which means that the result of the ITIL process serves as input for the ISO 27001 activities. There are different action items regarding countermeasures within the ITIL and ISO 27001 standards. So how can the company compliance still be assured after the mapping between the ITIL and ISO 27001 processes took place? It is a matter of compliance regarding the privacy and legislation of the involved participants and entities. ITIL and ISO 27001 have in common that they are both based on the Plan-Do-Check-Act (PDCA) model. From ITIL point of view, nearly all security controls in ISO 27001 are part of ITIL service management. It is also in the ITIL standard, chapter on service design that there is a reference on ISO 27001. The advantage of this approach is that the company's information security department is in line with the risk management department regarding which ITIL processes have been implemented through ISO 27001. The information security department can also easily identify which ISO 27001 objectives are already met through the use of ITIL and which still must be handled. Using this hybrid approach, considering ITIL and ISO 27001 together, companies can save a lot on time and money using mutual synergies and knowledge in this area. The need to use both standards at the same time is to establish a well-known information security process that covers all relevant aspects. If

doing so, a company can rely on acceptable security levels, effectively manage risks and reduce overall risk levels. We propose a mapping between ITIL and ISO 27001 action items based on the points in Sect. 3.1 and Sect. 3.2. Point 1 of ITIL, Define initial tasks for the roles is mapped to point 1 of ISO 27001, named Agree on an IT security policy. So starting with the initial tasks and roles, a security policy can be written and agreed on. The creation of an incident response system, point 2 of ITIL is the basis for establishing the position of a CISO in a company. So it is technical means, which is the base for organizational duties of a CISO position. Moreover, step 1 of ISO 27001, the establishment of a security policy is needed to have a CISO on duty. So there are not only relations between the standards but also within one standard. Point 3 of ITIL, the establishment of a monitoring system, serves as input for action item 5 of ISO 27001, ensuring effective risk management.

Only with a thorough configured monitoring and alerting system it is possible to conduct effective risk management. The goal is to mitigate risks and be aware of new risks. A classification of the monitored assets is important to easily identify the severity of an incident. Reaction times, escalation times, contact with partners and producers and time to recover are heavily dependant on the severity of an incident. The higher the severity is, the faster is the required reaction times, escalation times, communication with partners and producers and recovery time. Only if an organisation is certified in its core business areas, can it be able to embark upon business continuity and disaster recovery planning. Certified personnel as well as experience and knowledge in the matter of subjects are a plus. Input for this is the documentation of all necessary information and changes. The documentation must be extended and kept up to date at every chance. It is important to define boundaries to stakeholders and produce a control list consisting of action items as well. The boundaries to stakeholders serve as input for Annex A of the ISO 27001 standard.

## 5 High Availability Video Conferencing Service Provider

Our example is based on a high availability video conferencing service provider, who is supporting customers with their company video infrastructure. Thus it needs high availability and fast response times to the end client.

### 5.1 Instantiate the Cloud Pattern

To illustrate our approach, we use the example of a service provider. This company wants to offer video conferencing services to its customers. The video conferencing services are planned to be implemented via a cloud system.

Figure 2 shows an instance of the extended cloud pattern for the description in the following: The cloud provider is a company called Alpha. The main goal of the cloud provider is to maximize profit by maximizing the workload of the cloud. Therefore its sub-goals are to increase the number of cloud customers and their usage of the cloud, i.e. to increase the amount of data as well as the number and frequency of calculation

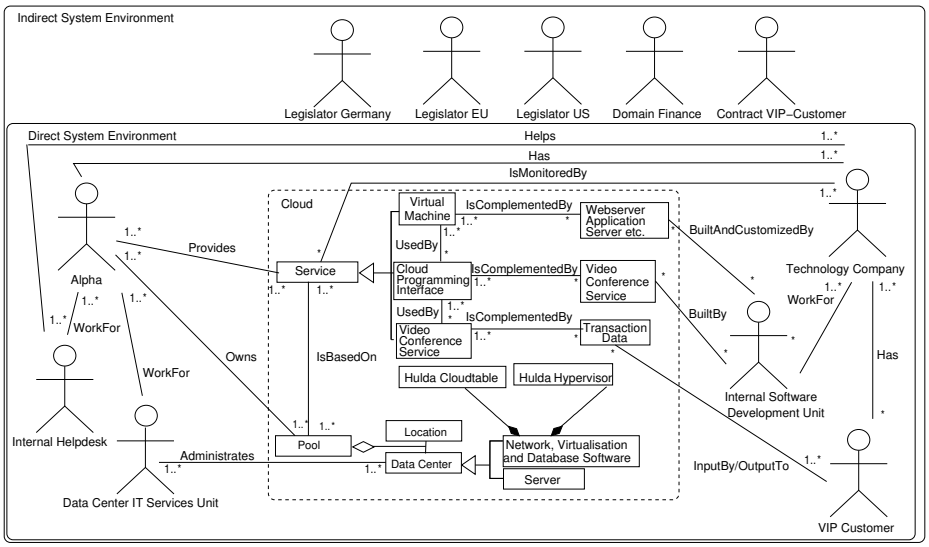


**Fig. 2.** Instantiated Cloud System Analysis Pattern with the Video Conferencing Scenario

activities. Fulfilling security requirements is only an indirect goal to acquire cloud customers and convince them to increase the subset of processes they outsource. The pool of the cloud is instantiated with Alpha's data centers that consist of servers, network, and virtualization software. The data centers are located in Germany and the US. Alpha uses the internal help desk of its data centre as cloud support and the internal data centre IT services unit as cloud administrator. Alpha implements the Alpha cloud table as cloud database and the Alpha hypervisor as cloud hypervisor. The cloud customer is instantiated with a technology company that plans to outsource the effected IT processes to the cloud to reduce costs and scale up their system for a broader number of end customers. Customer data such as IP addresses, names, and transaction log history are stored in the cloud. Transactions such as booked meetings are processed in the cloud. We instantiate the cloud developer with an internal software development unit of the technology company. This unit develops solutions for video conferencing in the cloud. The internal development unit installs and configures web- and application servers in virtual machines. The resulting cloud programming interface is the foundation for the video conferencing service. The technology company uses the cloud to conduct his/her financial business.

### 5.2 Describe relevant Business Processes

The business process in our scenario is made up of a cloud customer, who demands the service of a video conferencing suite, especially made for VIP customers. To maintain such a high available solution, the cloud customer requests the following services from

the cloud provider: A state of the art video conferencing system, using HD video quality and a fast and reliable connection between the video participants and conducting a penetration test against the video conferencing site once a year with a detailed report. The cloud customer network is maintained by the cloud provider, who is responsible for the security and non-disclosure of data. For HD video quality, the customer will need at least a 2 Mbit connection and preferably more bandwidth. It is also a good idea to have a single point of contact, globally reachable video support number that is used as the primary place to go for first level incidents. It is of course a good idea to have the WAN connections and the video conferencing service from the same cloud provider. There are not many providers who can offer both services on a worldwide basis. Once a week there needs to be ongoing discussion between the cloud provider and the customer concerning new video system installations and the incidents recorded at the first level support. The cloud provider is also responsible for keeping up maintenance and service contracts of the video endpoints. If the first level support is not successful or it takes too long a time to recover, the case is escalated to second and third level. The second level can be within the cloud provider or local IT at the customer site. The third level is the producer of the video equipment, which can be a partner of the cloud provider and/or customer. The customer needs proofed processes in place for scenarios, such as a video conference room installation or the hardware replacement of a video endpoint.

### 5.3 Describe Services in Detail

In our example, the video conferencing service is provided to the customers by the cloud provider. It consists of the dial-in bridge and one-to-one movie connections as well as security mechanisms. If a change occurs, such as that caused by the installation of a security update on the management server, customers are redirected to a backup system, which indicates that the main site is under maintenance and will be back in production soon. If an incident outside a maintenance window occurs, the responsible IT manager of the cloud customer will contact the service delivery manager of the cloud provider. The given incident has to be handled and restored to normal working conditions in accordance to the time frames specified in the agreed Key Performance Indicators (KPIs). If this is not possible, the cloud provider has to pay a penalty for the non delivery of the managed service. For the compliance with the KPIs, service reports with the availability expressed in percentage of the provided service are delivered to the customer. To further analyze the quality of the service, end-to-end monitoring from the customer network to the login server can be applied. The end-to-end monitoring reports can be accessed from the cloud customer via a separate web page. The task of the end-to-end monitoring is to supervise the availability and response time of the login service and alert the provider as well as the customer in case of exceeding defined thresholds. The system further distinguishes between warnings and errors and is capable of alerting status changes. The end-to-end monitoring procedure stimulates the user experience and does so by executing a macro of user transactions constantly 5 times per hour. The security requirements for the retrieval of these monitoring reports involve the use of certificates and encryption as well as a complex algorithm used for client authentication. This algorithm shall consist of a combination of 3 different authentication mechanisms.

First, the unique username, second user input by finishing a capture picture and third a unique password corresponding to the user. The certificate in use must be trusted by an authorized third party company, who issues the certificate and have an encryption standard of 256 bits. For VIP customers immersive, telepresence video rooms are used. This needs the involvement of different parties at the customer side, for example facility (cooling, heating, electrician,...) and the local video team. Once, all physical tasks have been carried out, the video system can be certified, prior to using it. The certification takes place between the customer site, who initiates a connection to the cloud provider and vice versa. Parts of this test includes presentation sharing, movement of people, taking a screenshot and having a stable connection for at least 15 minutes. The quality of the connection can be seen during the connection in the quality details. The technicians should have a look at parameters, such as delay, jitter and packet loss. A common issue can also be one way audio or video, which is mostly because of missing firewall configuration on one participant side.

### 5.4 Instantiate ISMS Policies

First an assessment is conducted by the cloud customer in order to select a cloud provider that best fits his requirements. Normally such a selection is done through a bidding procedure. The cloud customer is describing the services he wants to consume as well as availability values and response times for incidents. The cloud customer should also check if the cloud provider has a qualified 24x7 support team in place, which the customer can call, when there is a major incident or outage. Another important point is to clarify if the provided infrastructure is solely in use for the customer and not part of a multi tenant solution. Further, disaster recovery on the hardware side (e.g.: VMware HA, VMware Vmotion) and the existence of a fallback data centre should be clarified. It is also interesting in which country the data centre resides and where the customer data is actually stored. This is important as which national law applies and where the court jurisdiction resides. Which security mechanisms does the cloud provider have in use and which quality of cooling, electricity venues are in the field. It should also be clear, if the cloud provider will monitor the customer's servers and be responsible for data backups. Generally speaking, the service quality should be constantly monitored by the cloud provider. This can for instance be done with an end-to-end monitoring solution, where end user behavior is simulated. Such a solution measures the availability from the customer point of view as well as response times and network monitoring. End-to-end monitoring solutions are collating these KPIs through measuring scripts running on separate machines crawling through the productive environment. The monitoring results are then reported to the cloud customer once a month for every single service in use. The measurement criterion for the service delivery and maintenance duties are the KPI and are based on the overall availability, availability of customer processes and customer satisfaction. The monitoring results are to be delivered to the customer for quality assurance at the beginning of the month. For service delivery, references of customers (success stories), partner management (which partners support the cloud provider) and a sample contract can be requested. The contract duration, opt-out criterion as well as

price models for the services are necessary.

### 5.5 Conduct an internal and external Security Audit

The cloud provider of course will get the chance to improve their offer in the second phase. A feedback process from the cloud customer to the cloud provider after the first phase is recommended. The services provided to the customer are defined in a contract between the two parties involved. In this contract the service levels are expressed in SLA, as well as the response times during business hours and after business hours are defined. A high customer satisfaction rate is assured through security, availability and confidence in the cloud provider. The cloud provider has established processes and policies that maintain the security of the customer data. A confident handling of customer information and infrastructure is based on the consequent implementation of rules and processes, which are embedded in policies and specified in standards and operational guidelines. Implementing these guidelines is the duty of the cloud providers' employees. Based on these policies, responsibilities, roles, behavior, process definitions and supporting technologies are derived.

### 5.6 Implement Change Management

For the change log within the service delivery, all changes in the productive environment must be logged. The structure of the change log is as following: The first column is filled with an incremental ID, followed by the name of the change owner. The initiator of the change, which can vary, comes next. After that, the change cause, described in words or referring to a support ticket is listed. Next is the hostname, where the change is carried out, following the change description in descriptive language as well as the configuration changes itself in computer language. The category of the change is classified in regular, emergency and standard. It has to be defined, which duties belong to a standard change. If a change is non-standard, it is qualified by the engineer as a non-standard change. All productive changes have to be scheduled and appropriate configuration and fallback procedures in place prior to executing the change. The last possibility is a non-operational relevant change. This means changes in non productive environments and no scheduling of the change is needed. The risk of the change can vary from low to medium to high. At the end, a control check is performed, where the name of the change approver as well as the date the change was approved and the date the change was carried out, are documented. Last, but not least, a flag is inserted stating whether the change was successful or not. Changes are executed, following a four eye principle.With this feature, errors can be minimized and the overall availability and customer satisfaction is high. Urgent changes or emergency changes can be delivered faster, but require the consent of the Change Advisory Board (CAB).

## 6 Related Work

Calder [12] and Kersten et al. [13] provide advice for an ISO 27001 realisation. In addition, Klipper [14] focuses on risk management according to ISO 27005. This works do not consider relations to other standards like ITIL.

Cheremushkin et al. [15] [16] present a UML-based metamodel for several terms of the ISO 27000, e.g., assets. These meta-models can be instantiated and, thus, support the refinement process. However, the authors do not present a holistic approach to information security. The work mostly constructs models around specific terms in isolation. We support the establishment of an ISO 27001 ISMS using the processes in the ITIL standard.

Mondetino et al. investigate possible automation of controls that are listed in the ISO 27001 and ISO 27002 [17]. Their work can complement our own.

Fenz et al. [18] introduce an ontology-based framework for preparing ISO/IEC 27001 audits. They provide a rule-based engine which uses a security-ontology to determine if security requirements of a company are fulfilled. This work also does not consider the ITIL standard.

## 7 Conclusion and Future Work

We have established a method that helps with mapping ITIL action items to ISO 27001 action items. The method works in a compliant way, also after this mapping has been done. Our contribution is intended to help organisations, which are already certified or are thinking becoming certified.

Our approach offers the following main benefits:

- A structured method to map ITIL action items with ISO 27001 action items
- Systematic identification of relevant action items and determining compliance mechanisms for them
- Improving the outcome of business processes by adding benefits from mapping between standards
- Re-using the structured techniques of ITIL and ISO 27001 for supporting business processes in order to be compliant with current legislation and demands of law

As standardization is not an easy step for companies, we came up with suggested steps to help companies become certified. We presented a combination of technical and organizational means to master this process. Our cloud analysis pattern is the basis for the high availability video conferencing solution operating in the cloud. We apply our pattern on both, ITIL and ISO 27001 standards. Our hybrid approach, using the synergies from both certifications is shown in the mapping between them. In our example we present the whole life-cycle, the instantiation of the cloud pattern, the description of the relevant business processes, the description of the managed service in detail, the instantiation of ISMS policies, conducting internal and external securtity audits and finally, the implementation of change management within the organisation.

The work presented here is based on [5] and is further extended with the use of ITIL and our cloud- specific analysis pattern. Future work will involve the mastering of security and privacy questions within this context. The legislative framework in connection

with both the cloud provider and the customer side must be examined in more detail. We think that this paper builds a stable basis for all of these challenges.

## References


1. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee, G., Patterson, D.A., Rabkin, A., Stoica, I., Zaharia, M.: Above the clouds: A berkeley view of cloud computing. Technical report, EECS Department, University of California, Berkeley (2009)
2. Mell, P., Grance, T.: The NIST definition of cloud computing. Working Paper of the National Institute of Standards and Technology (NIST) (2009)
3. Vaquero, L.M., Rodero-Merino, L., Caceres, J., Lindner, M.: A break in the clouds: Towards a cloud definition. Special Interest Group on Data Communication (SIGCOMM) Computer Communication Review **39**(1) (2008) 50–55
4. Buyya, R., Ranjan, R., Calheiros, R.N.: Modeling and simulation of scalable cloud computing environments and the cloudsim toolkit: Challenges and opportunities. In: Proceedings of the International Conference von High Performance Computing and Simulation (HPCS), IEEE Computer Society (2009)
5. Beckers, K., Kuester, J., Faßbender, S., Schmidt, H.: Pattern-based support for context establishment and asset identification of the iso 27000 in the field of cloud computing. In: Proceedings of the International Conference on Availability, Reliability and Security (ARES), IEEE Computer Society (2011)
6. Jackson, M.: Problem Frames. Analyzing and structuring software development problems. Addison-Wesley (2001)
7. Fowler, M.: Analysis Patterns: Reusable Object Models. Addison-Wesley (1996)
8. Gamma, E., Helm, R., Johnson, R., Vlissides, J.: Design Patterns: Elements of Reusable Object-Oriented Software. Addison-Wesley (1994)
9. Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., Sommerlad, P.: Security Patterns: Integrating Security and Systems Engineering. Wiley (2006)
10. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC): Information technology - Security techniques - Information security management systems - Requirements. ISO/IEC 27001 (2005)
11. Government, H.: It infrastructure library (itil) (2012) `http://www.itil-officialsite.com/home/home.aspx`.
12. Calder, A.: Implementing Information Security based on ISO 27001/ISO 27002: A Management Guide. Haren Van Publishing (2009)
13. Kersten, H., Reuter, J., Schroeder, K.: ITSicherheitsmanagement nach ISO 27001 und Grundschutz. Vieweg+Teubner (2011)
14. Klipper, S.: Information Security Risk Management mit ISO/IEC 27005: Risikomanagement mit ISO/IEC 27001, 27005 und 31010. Vieweg+Teubner (2010)
15. Cheremushkin, D., Lyubimov, A.: An application of integral engineering technique to information security standards analysis and refinement. SIN '10 (2010)
16. Lyubimov, A., Cheremushkin, D., Andreeva, N., Shustikov, S.: Information security integral engineering technique and its application in isms design. In: Proceedings of the International Conference on Availability, Reliability and Security (ARES). (2011)
17. Montesino, R., Fenz, S.: Information security automation: how far can we go? In: Proceedings of the International Conference on Availability, Reliability and Security (ARES), IEEE Computer Society (2011)
18. Fenz, S., Goluch, G., Ekelhart, A., Riedl, B., Weippl, E.: nformation security fortification by ontological mapping of the iso/iec 27001 standard. In: Proceedings of the International Symposium on Dependable Computing, IEEE Computer Society (2007)