WHITE PAPER

Extending ITSM Capabilities to Include Information Security Management

Author:
Wouter Wyns
4me, Inc.

Author:
Geert Antheunis
Three Headed Giant

For more information visit: **4me.com**

WHITE PAPER

Extending ITSM Capabilities to Include Information Security Management

With the growing need for enterprises to comply with data protection legislation and security standards comes the need to set up a system to support and monitor the data protection and security procedures. This article investigates if it is a good idea to use the existing IT service management (ITSM) system or enterprise service management (ESM) system for this purpose and identifies the functionality an ITSM system should have to be successful in this domain.

Introduction

IT is not an island. Nor is IT security. As any good management framework will tell you, Governance, Risk and Compliancy (GRC) lies at the heart of what we do in IT. We want to make sure to do the right things, and to do them right. That may sound simple, but it is easy to get lost in the myriad of frameworks, best practices, guidelines, standards and general good advice out there. And when you have finally identified the management frameworks your organization wants to adhere to, you need to decide on the system or systems to manage the frameworks. Or as is so often the case, organizations just end up with a separate management system for each of these frameworks.

Would it not be better to have one management system, a so-called Integrated Management System (IMS) that combines all aspects of an organization's systems, processes and standards into one smart system? And why not use your existing IT service management system or enterprise management system to that purpose? This one blended system will allow your organization to streamline its management, save time and increase efficiency.

To successfully bring the management frameworks on one management system, a first important question to be answered is whether there is any common ground to all these frameworks. And if indeed these frameworks share some common principles, does this mean that it is a good idea to use one common system to support and monitor these frameworks? And secondly, what are the requirements for this integrated management system and does your current ITSM system comply with these requirements?

This white paper will answer both questions.

A Focus on ISO Standards

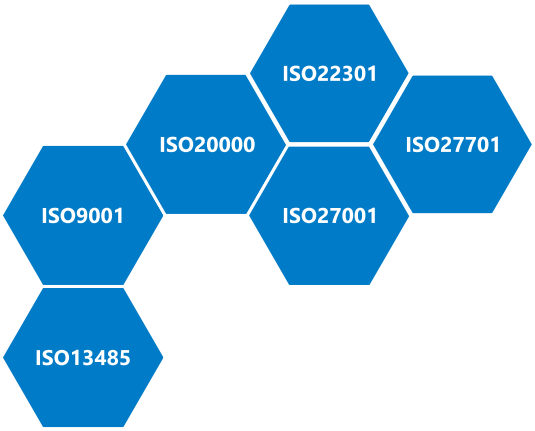
The first thing to understand is that every management framework serves a different use and purpose. CobIT, for example, is an excellent framework that gives an IT department a fairly good idea of WHAT they should be doing. From high level business alignment down to the nitty gritty of being able to process service requests. Then there are frameworks such as ITIL that help define HOW to achieve those objectives. These bodies of knowledge are full of best practices and guidance for designing, implementing and maintaining a set of processes and procedures. To evaluate if the right things are done in the right way, you need an independent touchstone, a benchmark that can provide QUALITY assurance. That is where standards and certifications come in.

This white paper will focus on the different ISO/IEC standards, which have a lot in common. However, this doesn't mean that the conclusions are limited to those standards. There are other assurance mechanisms like SOC 2 and, depending on your region, these may even be valued more than an ISO27001 certification. These frameworks may have a slightly different approach, but they also have a lot of similarities. So, although this article will focus on the ISO/IEC standard approach for management systems, the core of the message remains the same: leverage your efforts to maximum capacity.

An Overview of Common ISO Standards

ISO 27001

The best-known standard for information security is ISO 27001. This standard explains how to establish, implement, operate, monitor, review, maintain and improve an Information Security Management System. In addition, it specifies 35 control objectives and 115 controls that an organization can implement to improve its information security.



ISO 27701

Just over 2 years ago, the General Data Protection Regulation (GDPR) came into force. Since then, any organization that handles personal data from EU citizens should be compliant with this regulation. Many organizations turned to ISO 27001 for this, but privacy is more than just Information Security. It raises other questions and introduces new risks. That is why last year ISO 27701 was introduced. It is an extension of the 27001 standard and explains how to establish, implement, operate, monitor, review, maintain and improve a Privacy Information Management System. These high-level activities (establish, implement, operate, monitor, review, maintain and improve) recur in these ISO frameworks.

ISO 20000

For IT service management ISO 20000 is the standard. Like the other ISO standards it includes the same high-level activities.

ISO 22301

Another ISO standard that has proven to be useful during the global pandemic is ISO 22301. This standard specifies the requirements for a Business Continuity Management System to protect organizations against, reduce the likelihood of occurrence of, prepare for, respond to, and recover from disruptive incidents when they arise.

There is no denying that the COVID-19 pandemic was very disruptive and changed the way we work for a lot of people. We expect this standard to attract more attention over the coming years because it always takes some defining moment, like the introduction of GDPR or COVID-19, to create enough traction to change things. Coincidentally, business continuity was originally part of the 27001 standard as well, but it was deemed important enough to merit its own standard. There is still a little business continuity left in the controls of ISO 27001, but the bulk has shifted to ISO 22301.

ISO 9001

The one standard that we probably all know is the ISO 9001 standard that sets requirements for a Quality Management System. It makes a lot of sense to apply quality principles to all activities we perform as businesses. Organizations are probably applying many best practices in this field already. Therefore, it might not be a bad idea to look at this standard and assess where you stand as a company in the field of quality.

Common Elements of Different ISO Standards

Over the years, the International Standards Organization (ISO) has realized that there are a lot of similarities between the different management system standards and has been working to achieve a common language and structure between them. The common language starts with the list of high-level activities (establish, implement, operate, monitor, review, maintain and improve) to be performed. But there are more similarities.

The Same Structure

All ISO management system standards must follow the same structure. This is defined in the High-Level Structure (HLS), a set of 10 clauses that all ISO management system standards are required to use. This HLS structure is much more than just applying the same look and feel. It should enable greater integration between systems of different disciplines.

The first three clauses are: 1. The Scope, 2. The Normative References and 3. Terms and Definitions. They provide information that is specific to each framework and offer no common ground. So let us have a closer look at clauses 4 to 10, which contain the mandatory requirements. These clauses are:

4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

These elements are really the foundation of a management system. It is clear that whichever management system is implemented in an organization, the context of the organization and the leadership are the same. It is necessary to establish all these clauses for every management system that is used. When this groundwork has been done for one management system, it will probably have covered a lot of ground required for another management system. Aside from the structure, let us also look at some other common aspects that will benefit from an integrated management system.

Bundling Forces in an Integrated Management System

Bringing management frameworks together in an integrated management system is also about bundling forces. The benefits of this become clear in the following areas:

Raising Risk Awareness

Raising risk awareness is a substantial factor to achieve results, whether you are introducing the concept of a Change Advisory Board, or teaching staff what to do in case of a data breach. Training people in what to do and changing their attitude and behavior is a challenge for management, but one that is vital because we are tackling the people factor here, and implementing a management system is above all a people project.

An integrated management system will not tackle this challenge. When awareness is an obstacle, it is a good idea to consider what 'no awareness' means in terms of 'lack of ...': 'lack of interest' and 'lack of leadership', but also 'lack of knowledge sharing among organizational boundaries' and 'lack of coordination'. While an integrated management system will not resolve the lack of awareness, it can certainly help to remove some of the obstacles.

Logging, Monitoring, Performance Analysis

Logging, monitoring, performance analysis, KPI's, ... These are all things that are very familiar to IT service management professionals. And by combining expertise in ISO 20000 (for IT service management) with elements from other management systems you will be able to do better still.

Internal Audit and Management Review

ISO 27001 adds two important concepts that are also very interesting in a service management context. The first is the requirement for an organization to set up an internal audit program for the management system. Think of Continual Improvement in the Information Technology Infrastructure Library (ITIL), established as a function. This concept fits very well within ITSM, especially when combining fields like services, operations, quality, security, privacy and business continuity. When done right this internal audit function becomes a significant contributor to improvements, both internally and externally.

The second concept from ISO 27001 is the Management Review. In ITIL, there is one risk that is repeated over and over when talking about the risks to any of the processes: "Lack of management commitment". At a certain point, this risk has become the most common excuse to explain failure. ISO27001 gently forces management to take responsibility by making sure there is a process in place. Once this process is established, senior management will become aware of the scope and objectives of the management system and of the benefits it brings. And more importantly: it lets management actively reiterate their commitment at regular intervals.

Control objectives and controls

Looking at the control objectives and controls itself, it is clear that service management can bring a lot to the table. There is a lot more guidance in ISO 20000 and ITIL on how to address controls like Incident Management and Change Management. A good example is Annex A.16.1 of ISO 27001, about managing information security incidents, events and weaknesses. Implementing these incident management security procedures without a liaison or without checking the maturity of the current IT Incident Management would be a real shame. In fact, an organization should always start from what is already in place in terms of Incident Management, Change Management, CMDB, or Problem Management, and work out what requirements are missing and what you need to add in terms of security or privacy. They should not be treated as separate projects or processes!

6 Requirements for an Integrated Management System

By now, it is clear that there are many theoretical and practical reasons to create an integrated management system on top of the existing IT or enterprise service management system.

The next question is whether the existing IT service management system is fit to support GRC and quality control frameworks. Below we will explore 6 requirements a service management system should comply with to become a real integrated management system.

Data Segregation

Data confidentiality is definitely one of the pillars of information security. And there is also segregation of duties, which is an important requirement in ISO standards. This all means that a service management system needs multi-tenancy capabilities to segregate data and functions. For example: when a laptop is stolen or lost, a ticket will be registered in the ITSM system to replace the laptop. When sensitive data is stored on the laptop and there is a chance that access to the laptop was not well secured (e.g., password written on a note in the laptop bag), a data breach incident must be registered and processed by the data protection team. This ticket should not be visible to the IT people: it can contain information regarding the sensitive data that has been lost which should not be shared with all IT specialists.

Auditable Workflows and Recurrent Tasks

When implementing GRC and quality control frameworks, an organization needs proof of compliance or a certificate at a certain point. That is where external auditors come in. Their job is to find evidence between what an organization says it does and what actually happens. An auditor is not there to look for faults or inconsistencies; they take an objective look based on the evidence they find.

Recurring tasks are a powerful means to implement what has been specified in the controls and to provide proof of compliance. For example, when the security policy includes the rule that any IT specialist needs to complete the Information Security Training every 6 months, it is a good idea to define a recurring task for this activity that will be assigned to each of the IT specialists.

Workflows are required to support the steps described in the security response plans. For example, a data breach response plan that describes the steps to be taken when a data breach happens should be supported by a workflow with a task for each of these steps.

These recurring tasks and workflows need to be auditable: the service management system will provide all the information on who has done what and when. The external auditors will love these features: it provides them with all the evidence they seek.

Target Dates and SLAs

Most data protection and security regulations include some target dates that can lead to serious fines when violated. For example, GDPR introduces a duty on all organizations to report certain personal data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach. The service management system needs an efficient functionality to define and monitor these target dates.

Enterprise Service Management

Security is everyone's responsibility. A good starting point is the Self Service portal of the enterprise service management system that is published to internal and external users. The enterprise Self Service portal gives access to information about and the ability to submit requests to all support domains (e.g. IT, HR, Facilities, Customer Services, Partner Management) that provide service to a given end-user. Security and data protection must be part of this and should get a prominent place. An enterprise service management portal can provide great support in creating security awareness.
It can give all users one-click access to the security and data protection domain.

Security is not a silo or an island. Enterprise Management System makes sure that these different support domains can collaborate and use the same data, when allowed, or use their own data when necessary. The overarching process can be defined so that the desired outcomes can be consistently delivered.

Asset Inventory and Risk Register

According to ISO 27001, an asset inventory needs to be defined, assets being anything that brings value to the organization. These include Hardware, Software, Information, Infrastructure, People and Outsourced services. And these assets are the key element of identifying risks. Therefore, the service management system should have the functionality to register these assets, link them to an asset owner (who is responsible for the asset?) and provide the functionality to create a risk register with links to these assets. This Risk register is the glue between the Management Systems.

Dashboard and reporting

Finally, dashboarding and reporting are essential for both IT Service Management and Information Security Management to be effective. Whether it is an operational dashboard steering day-to-day operations or historical reporting used for sampling by an auditor.

Conclusion

There are many benefits in adopting an integrated approach and blending the IT service management system and IT security system together. Not only will organizations be making more efficient use of their resources, but they will also reduce complexity instead of increasing it. And by defining a common language and approach towards risk management, there will be a clearer understanding of the context of the organization and the needs and expectations of interested parties.

Organizations should not try to create a different process for a regular Incident, a Security Incident, or a Data Breach. Instead, they should be treated in a consistent and flexible process flow that allows the people and teams in the organization to collaborate by using the same tools and using the same language.

But make sure the service management system fits with the requirements for an Integrated Management System. An organization will need solid data segregation to protect the sensitive information that is typically stored in security incidents.

About 4me

4me® combines ITSM with ESM and SIAM capabilities making it possible for all internal departments, such as IT, HR and Facilities, to work seamlessly with each other, as well as with external managed service providers.

About 3 Headed Giant

Three Headed Giant (3HG) specializes in Enterprise Service Management. We offer innovative out-of-the box and tailor-made solutions that help our customers to organise their service delivery efficiently and effectively. Our approach is pragmatic, result driven and aims to offer real value for our customers. We want to be recognized as a knowledge organisation with a proven track record that is fueled by our enthusiastic and committed consultants that can make a difference out there.

For more information visit: **4me.com**