ITIL security management

The **ITIL security management** process describes the structured fitting of security in the management organization. ITIL security management is based on the ISO 27001 standard. According to ISO.ORG [1] "ISO/IEC 27001:2005 covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations). ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. ISO/IEC 27001:2005 is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties."

A basic concept of security management is the information security. The primary goal of information security is to guarantee safety of information. When protecting information it is the value of the information that must be protected. These values are stipulated by the confidentiality, integrity and availability. Inferred aspects are privacy, anonymity and verifiability.

The goal of the Security Management is split up in two parts:

1. The realization of the security requirements defined in the service level agreement (SLA) and other external requirements which are specified in underpinning contracts, legislation and possible internal or external imposed policies.
2. The realization of a basic level of security. This is necessary to guarantee the continuity of the management organization. This is also necessary in order to reach a simplified service-level management for the information security, as it happens to be easier to manage a limited number of SLAs than it is to manage a large number of SLAs.

The input of the security management process is formed by the SLAs with the specified security requirements, legislation documents (if applicable) and other (external) underpinning contracts. These requirements can also act as key performance indicators (KPIs) which can be used for the process management and for the justification of the results of the security management process.

The output gives justification information to the realization of the SLAs and a report with deviations from the requirements.

The security management process has relations with almost all other ITIL-processes. However, in this particular section the most obvious relations will be the relations to the service level management process, the incident management process and the Change Management process.

The security management process

The security management process consists of activities that are carried out by the security management itself or activities that are controlled by the security management.

Because organizations and their information systems constantly change, the activities within the security management process must be revised continuously, in order to stay up-to-date and effective. Security management is a continuous process and it can be compared to W. Edwards Deming's Quality Circle (Plan, Do, Check, Act).

The inputs are the requirements which are formed by the clients. The requirements are translated into security services, security quality that needs to be provided in the security section of the service level agreements. As you can see in the picture there are arrows going both ways; from the client to the SLA; from the SLA to the client and from the SLA to the plan sub-process; from the plan sub-process to the SLA. This means that both the client and the plan sub-process have inputs in the SLA and the SLA is an input for both the client and the process. The provider then develops the security plans for his/her organization. These security plans contain the security policies and the

operational level agreements. The security plans (Plan) are then implemented (Do) and the implementation is then evaluated (Check). After the evaluation then both the plans and the implementation of the plan are maintained (Act).

The activities, results/products and the process are documented. External reports are written and sent to the clients. The clients are then able to adapt their requirements based on the information received through the reports. Furthermore, the service provider can adjust their plan or the implementation based on their findings in order to satisfy all the requirements stated in the SLA (including new requirements).

Control

The first activity in the security management process is the “Control” sub-process. The Control sub-process organizes and manages the security management process itself. The Control sub-process defines the processes, the allocation of responsibility for the policy statements and the management framework.

The security management framework defines the sub-processes for: the development of security plans, the implementation of the security plans, the evaluation and how the results of the evaluations are translated into action plans. Furthermore, the management framework defines how should be reported to clients.

The activities that take place in the Control process are summed up in the following table, which contains the name of the (sub) activity and a short definition of the activity.

Activities	Sub-Activities	Descriptions
Control	Implement policies	This process outlines the specific requirements and rules that have to be met in order to implement security management. The process ends with *policy statement*.
	Set up the security organization	This process sets up the organizations for information security. For example in this process the structure the responsibilities are set up. This process ends with *security management framework*.
	Reporting	In this process the whole targeting process is documented in a specific way. This process ends with *reports*.

The meta-modeling technique was used in order to model the activities of the control sub-process. The following figure is the meta-process model of the control sub-process. It is based on a UML activity diagram and it gives an overview of the activities of the Control sub-process. The grey rectangle represents the control sub-process and the smaller beam shapes inside of the grey rectangle represent the activities that take place inside the control sub-process. The beams with a black shadow indicate that the activity is a closed (complex) activity. This means that the activity consists of a collection of (sub) activities but these activities are not expanded because they are not relevant in this particular context. The white beam without shadow indicates that the reporting activity is a standard activity. This means that reporting does not contain (sub) activities.

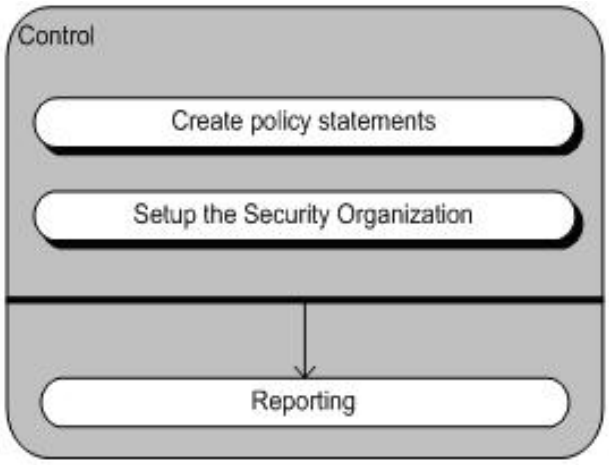

Figure 2.1.1: Meta-process model Control sub-process

Furthermore, it is noticeable that the first two activities are not linked with an arrow and that there is a black stripe with an arrow leading to the reporting activity. This means that the two first activities are not sequential. They are

unordered activities and after these two activities have taken place the reporting activity will sequentially follow. For a more extensive explanation of the meta-modeling technique consult the Meta-modeling wiki.

The following table (table 2.1.2) is a concept definition table.

Concept	Description
CONTROL DOCUMENTS	CONTROL is a description of how SECURITY MANAGEMENT will be organized and how it will be managed.
POLICY STATEMENTS	POLICY STATEMENTS are documents that outlines specific requirements or rules that must be met. In the information security realm, policies are usually point-specific, covering a single area. For example, an “Acceptable Use” policy would cover the rules and regulations for appropriate use of the computing facilities.
SECURITY MANAGEMENT FRAMEWORK	SECURITY MANAGEMENT FRAMEWORK is an established management framework to initiate and control the implementation of information security within your organization and to manage ongoing information security provision.

Table 2.1.2: Concept and definition control sub-process Security management

The meta-data model of the control sub-process is based on a UML class diagram. In figure 2.1.2 is the meta-data model of the control sub-process.

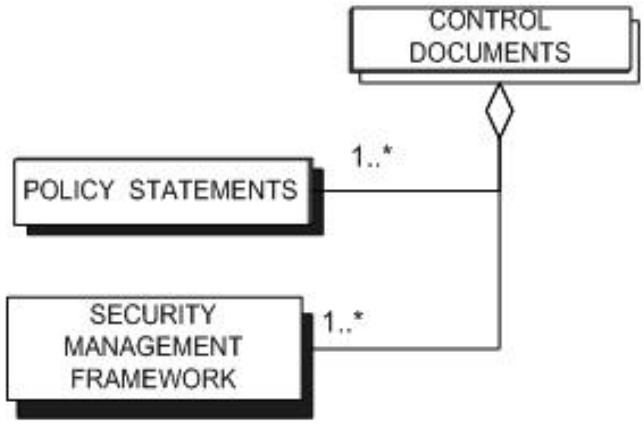

Figure 2.1.2: Meta-process model control sub-process

The CONTROL rectangle with a white shadow is an open complex concept. This means that the CONTROL rectangle consists of a collection of (sub) concepts and these concepts are expanded in this particular context.

The following picture (figure 2.1.3) is the process-data model of the control sub-process. This picture shows the integration of the two models. The dotted arrows indicate which concepts are created or adjusted in the corresponding activities.

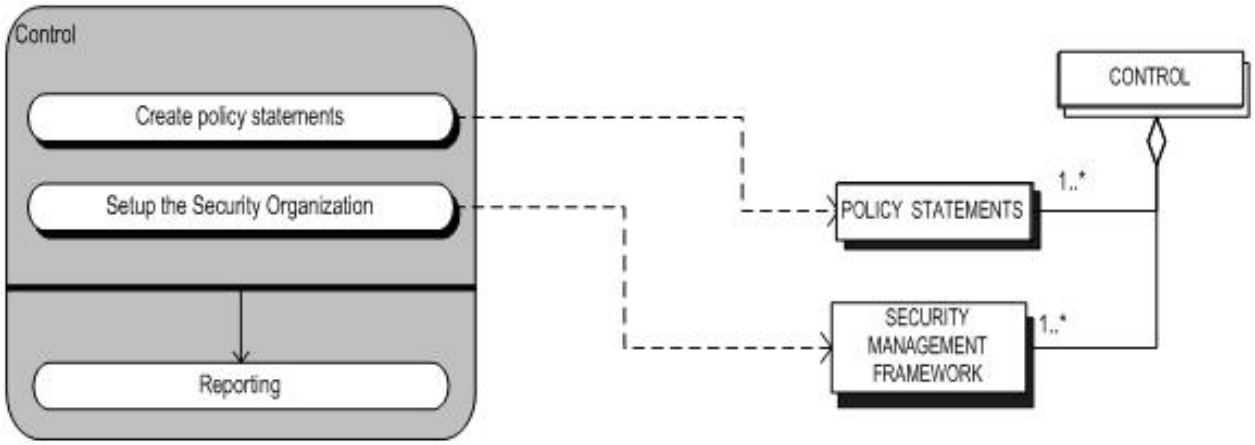

Figure 2.1.3: Process-data model control sub-process

Plan

The Plan sub-process contains activities that in cooperation with the Service Level Management lead to the (information) Security section in the SLA. Furthermore, the Plan sub-process contains activities that are related to the underpinning contracts which are specific for (information) security.

In the Plan sub-process the goals formulated in the SLA are specified in the form of Operational Level Agreements (OLA). These OLA's can be defined as security plans for a specific internal organization entity of the service provider.

Besides the input of the SLA, the Plan sub-process also works with the policy statements of the service provider itself. As said earlier these policy statements are defined in the control sub-process.

The Operational Level Agreements for information security are set up and implemented based on the ITIL process. This means that there has to be cooperation with other ITIL processes. For example if the security management wishes to change the IT infrastructure in order to achieve maximum security, these changes will only be done through the Change Management process. The Security Management will deliver the input (Request for change) for this change. The change Manager is responsible for the Change Management Process itself.

Table 2.3.1 shows the activity plan the (sub) activities and their definition.

Activities	Sub-Activities	Descriptions
Plan	Create Security section for SLA	This process contains activities that lead to the security agreements paragraph in the service level agreements. At the end of this process the *Security* section of the service level agreement is created.
	Create underpinning Contracts	This process contains activities that lead to UNDERPINNING CONTRACTS. These contracts are specific for security.
	Create Operational level agreements	The general formulated goals in the SLA are specified in operational level agreements. These agreements can be seen as security plans for specific organization units.
	Reporting	In this process the whole Create plan process is documented in a specific way. This process ends with REPORTS.

Table 2.2.1: (Sub) activities and descriptions Plan sub-process ITIL Security Management

As well as for the Control sub-process the Plan sub-process has been modeled using the meta-modeling technique. On the right side of figure 2.2.1 the meta-process model of the Plan sub-process is given.

As you can see the Plan sub-process consists of a combination of unordered and ordered (sub) activities. Furthermore, it is noticeable that the sub-process contains three complex activities which are all closed activities and one standard activity. Table 2.2.1 consists of concepts that are created or adjusted during the plan sub-process. The table also gives a definition of these concepts.

Concept	Description
PLAN	Formulated schemes for the security agreements.
Security section of the security level agreements	The security agreements paragraph in the written agreements between a Service Provider and the customer(s) that documents agreed Service Levels for a service.
UNDERPINNING CONTRACTS	A contract with an external supplier covering delivery of services that support the IT organisation in their delivery of services.
OPERATIONAL LEVEL AGREEMENTS	An internal agreement covering the delivery of services which support the IT organization in their delivery of services.

Table 2.2.2: Concept and definition Plan sub-process Security management

Just as the Control sub-process the Plan sub-process is modeled using the meta-modeling technique. The left side of figure 2.2.1 is the meta-data model of the Plan sub-process.

The Plan rectangle is an open (complex) concept which has an aggregation type of relationship with two closed (complex) concepts and one standard concept. The two closed concepts are not expanded in this particular context.

The following picture (figure 2.2.1) is the process-data diagram of the Plan sub-process. This picture shows the integration of the two models. The dotted arrows indicate which concepts are created or adjusted in the corresponding activities of the Plan sub-process.

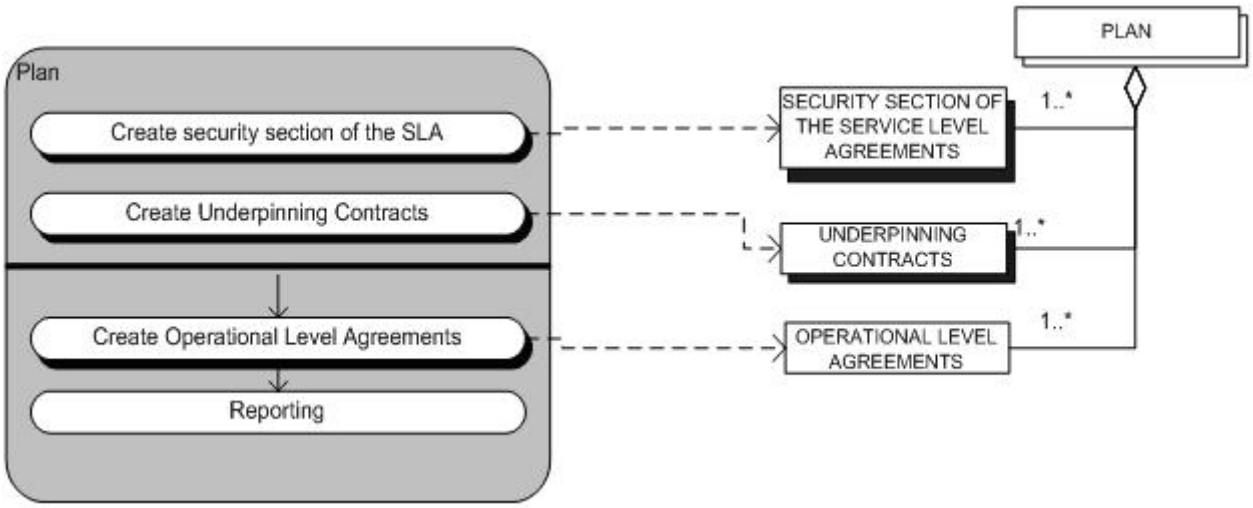

Figure 2.2.1: Process-data model Plan sub-process

Implementation

The Implementation sub-process makes sure that all measures, as specified in the plans, are properly implemented. During the Implementation sub-process no (new) measures are defined nor changed. The definition or change of measures will take place in the Plan sub-process in cooperation with the Change Management Process.

The activities that take place in the implementation sub-process are summed up in the following table (table 2.3.1). The table contains the name of the (sub) activity and a short definition of the activity.

Activities	Sub-Activities	Descriptions
Implement	Classifying and managing of IT applications	Process of formally grouping *configuration items* by type, e.g., software, hardware, documentation, environment, application. Process of formally identifying changes by type e.g., project scope change request, validation change request, infrastructure change request this process leads to *asset classification and control documents*.
	Implement personnel security	Here measures are adopted in order to give personnel safety and confidence and measures to prevent a crime/fraud. The process ends with *personnel security*.
	Implement security management	In this process specific security requirements and/or security rules that must be met are outlined and documented. The process ends with *security policies*.
	Implement access control	In this process specific access security requirements and/or access security rules that must be met are outlined and documented. The process ends with *access control*.
	Reporting	In this process the whole *implement as planned process* is documented in a specific way. This process ends with *reports*.

Table 2.3.1: (Sub) activities and descriptions Implementation sub-process ITIL Security Management

The left side of figure 2.3.1 is the meta-process model of the Implementation phase. The four labels with a black shadow mean that these activities are closed concepts and they are not expanded in this context. It is also noticeable that there are no arrows connecting these four activities this means that these activities are unordered and the reporting will be carried out after the completion of al the four activities.

During the implementation phase there are a number of concepts that are created and /or adjusted. See table 2.3.2 for an overview of the most common concepts and their description.

Concept	Description
Implementation	Accomplished security management according to the security management plan.
Asset classification and control documents	A comprehensive inventory of assets with responsibility assigned to ensure that effective security protection is maintained.
Personnel security	Well defined job descriptions for all staff outlining security roles and responsibilities.
Security policies	Security policies are documents that outlines specific security requirements or security rules that must be met.
Access control	Network management to ensure that only those with the appropriate responsibility have access to information in the networks and the protection of the supporting infrastructure.

Table 2.3.2: Concept and definition Implementation sub-process Security management

The concepts created and/or adjusted are modeled using the meta-modeling technique. The right side of figure 2.3.1 is the meta-data model of the implementation sub-process.

The implementation documents are an open concept and is expanded upon in this context. It consists of four closed concepts which are not expanded because they are irrelevant in this particular context.

In order to make the relations between the two models clearer the integration of the two models are illustrated in figure 2.3.1. The dotted arrows running from the activities to the concepts illustrate which concepts are created/ adjusted in the corresponding activities.

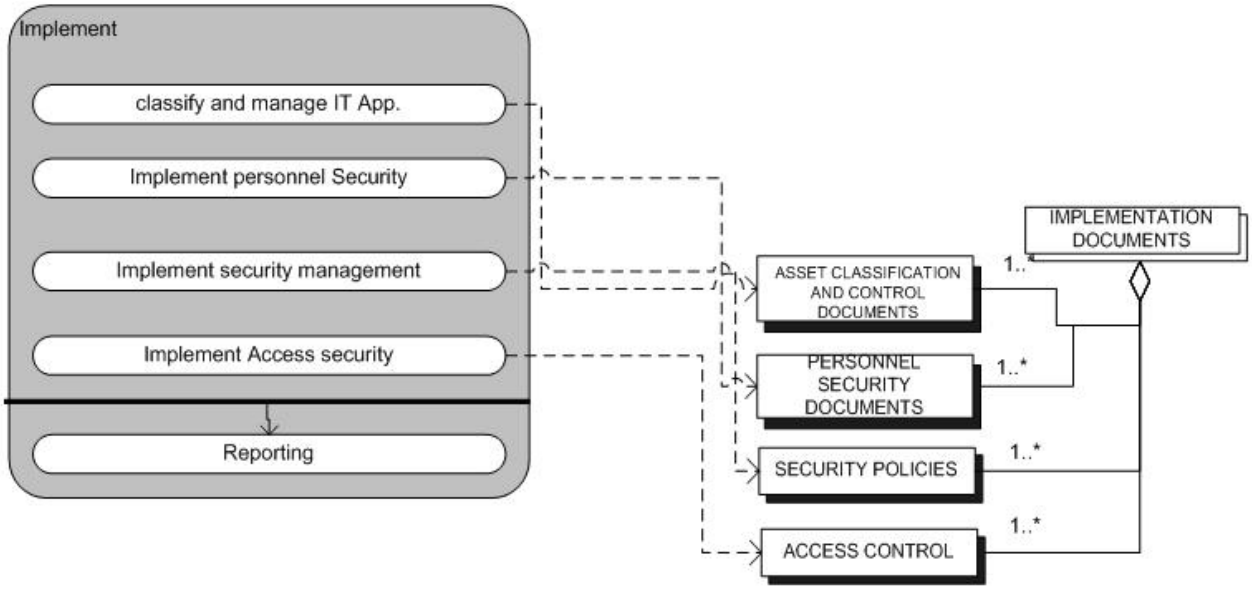

Figure 2.3.1: Process-data model Implementation sub-process

Evaluation

The evaluation of the implementation and the plans is very important. The evaluation is necessary to measure the success of the implementation and the Security plans. The evaluation is also very important for the clients (and possibly third parties). The results of the Evaluation sub-process are used to maintain the agreed measures and the implementation itself. Evaluation results can lead to new requirements and so lead to a Request for Change. The request for change is then defined and it is then send to the Change Management process.

Mainly there are three sorts of evaluation; the Self-assessment; internal audit, and external audit.

The self-assessment is mainly carried out in the organization of the processes. The internal audits are carried out by internal IT-auditors and the external audits are carried out by external independent IT-auditors. Besides, the

evaluations already mentioned an evaluation based on the communicated security incidents will also take place. The most important activities for this evaluation are the security monitoring of IT-systems; verify if the security legislation and the implementation of the security plans are complied; trace and react to undesirable use of the IT-supplies.

The activities that take place in the evaluation sub-process are summed up in the following table (Table 2.4.1). The table contains the name of the (sub) activity and a short definition of the activity.

Activities	Sub-Activities	Descriptions
Evaluate	Self-assessment	In this process an examination of the implemented security agreements is done by the organization of the process itself. The result of this process is SELF ASSESSMENT DOCUMENTS.
	Internal Audit	In this process an examination of the implemented security agreements is done by an internal EDP auditor. The result of this process is INTERNAL AUDIT.
	External audit	In this process an examination of the implemented security agreements is done by an external EDP auditor. The result of this process is EXTERNAL AUDIT.
	Evaluation based on security incidents	In this process an examination of the implemented security agreements is done based on security events which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service. The result of this process is SECURITY INCIDENTS.
	Reporting	In this process the whole Evaluate implementation process is documented in a specific way. This process ends with REPORTS.

Table 2.4.1: (Sub) activities and descriptions Evaluation sub-process ITIL Security Management

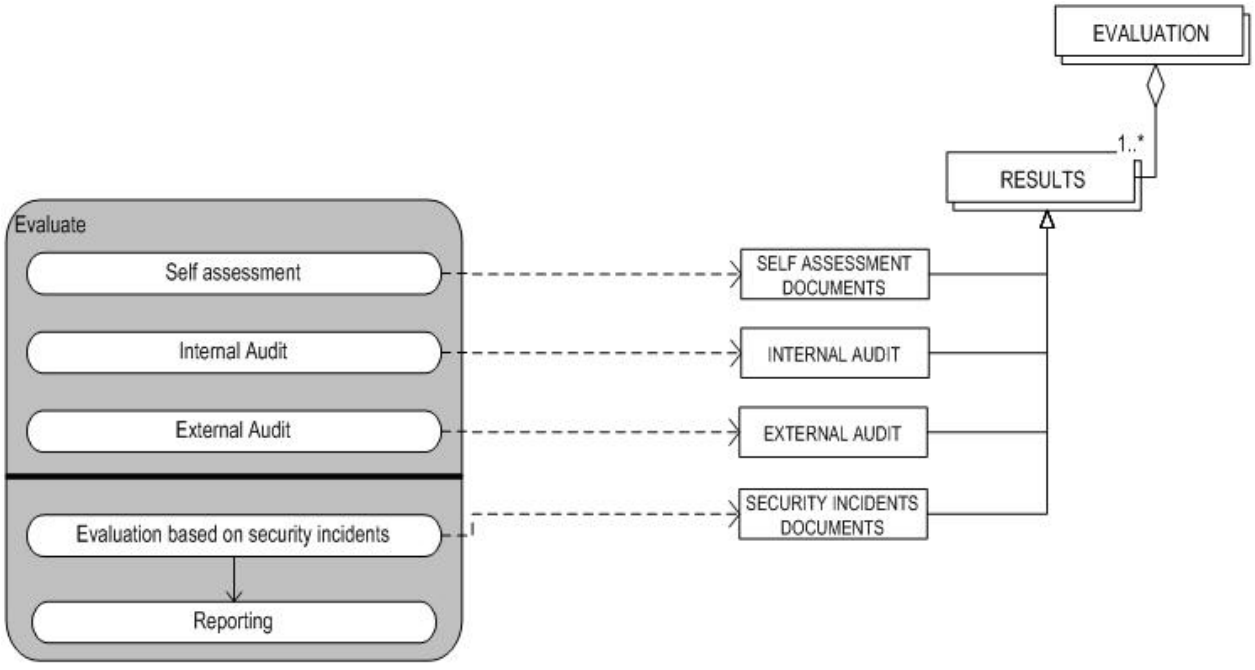

Figure 2.4.1: Process-data model Evaluation sub-process

The process-data diagram illustrated in the figure 2.4.1 consists of a meta-process model and a meta-data model. The Evaluation sub-process was modeled using the meta-modeling technique. The dotted arrows running from the meta-process diagram (left) to the meta-data diagram (right) indicate which concepts are created/ adjusted in the corresponding activities. All of the activities in the evaluation phase are standard activities. For a short description of the Evaluation phase concepts see Table 2.4.2 where the concepts are listed and defined.

Concept	Description
EVALUATION	Evaluated/checked implementation.
RESULTS	The outcome of the evaluated implementation.
SELF ASSESSMENT DOCUMENTS	Result of the examination of the security management by the organization of the process itself.
INTERNAL AUDIT	Result of the examination of the security management by the internal EDP auditor.
EXTERNAL AUDIT	Result of the examination of the security management by the external EDP auditor.
SECURITY INCIDENTS DOCUMENTS	Results of evaluating security events which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service.

Table 2.4.2: Concept and definition evaluation sub-process Security management

Maintenance

It is necessary for the security to be maintained. Because of changes in the IT-infrastructure and changes in the organization itself security risks are bound to change over time. The maintenance of the security concerns both the maintenance of the security section of the service level agreements and the more detailed security plans.

The maintenance is based on the results of the Evaluation sub-process and insight in the changing risks. These activities will only produce proposals. The proposals serve as inputs for the plan sub-process and will go through the whole cycle or the proposals can be taken in the maintenance of the service level agreements. In both cases the proposals could lead to activities in the action plan. The actual changes will be carried by the Change Management process. For more information about the Change Management Process consult the Change Management Wiki.

The activities that take place in the maintain sub-process are summed up in the following table (Table 2.5.1). The table contains the name of the (sub) activity and a short definition of the activity.

Activities	Sub-Activities	Descriptions
Maintain	Maintenance of Service level agreements	This is a process to keep the service level agreements in proper condition. The process ends with MAINTAINED SERVICE LEVEL AGREEMENTS.
	Maintenance of operational level agreements	This is a process to keep the operational level agreements in proper condition. The process ends with MAINTAINED OPERATIONAL LEVEL AGREEMENTS.
	Request for change to SLA and/or OLA	Request for a change to the SLA and/or OLA is formulated. This process ends with a REQUEST FOR CHANGE.
	Reporting	In this process the whole maintain implemented security policies process is documented in a specific way. This process ends with REPORTS.

Table 2.5.1: (Sub) activities and descriptions Maintenance sub-process ITIL Security Management

Figure 2.5.1 is the process-data diagram of the implementation sub-process. This picture shows the integration of the meta-process model (left) and the meta-data model (right). The dotted arrows indicate which concepts are created or adjusted in the activities of the implementation phase.

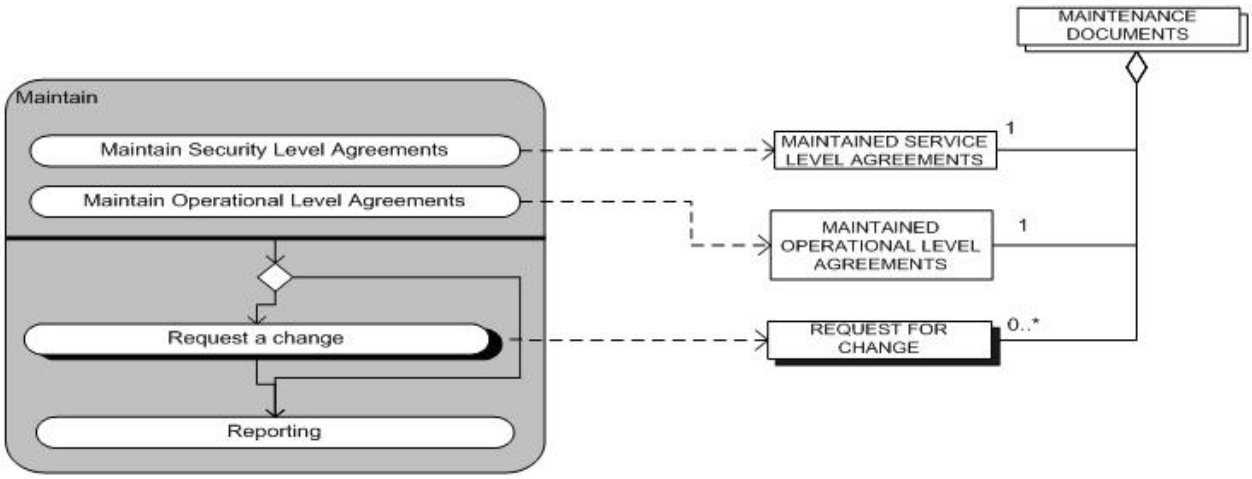

Figure 2.5.1: Process-data model Maintenance sub-process

The maintenance sub-process starts with the maintenance of the service level agreements and the maintenance of the operational level agreements. After these activities take place (in no particular order) and there is a request for a change the request for change activity will take place and after the request for change activity is concluded the reporting activity starts. If there is no request for a change then the reporting activity will start directly after the first two activities. The concepts in the meta-data model are created/ adjusted during the maintenance phase. For a list of the concepts and their definition take a look at table 2.5.2.

Concept	Description
MAINTENANCE DOCUMENTS	Agreements kept in proper condition.
MAINTAINED SERVICE LEVEL AGREEMENTS	Service Level Agreements(security paragraph) kept in proper condition.
MAINTAINED OPERATIONAL LEVEL AGREEMENTS	Operational Level Agreements kept in proper condition.
REQUEST FOR CHANGE	Form, or screen, used to record details of a request for a change to the SLA/OLA.

Table 2.5.2: Concept and definition Plan sub-process Security management

Complete process-data model

The following picture shows the complete process-data model of the Security Management process. This means that the complete meta-process model and the complete meta-data model and the integrations of the two models of the Security Management process are shown.

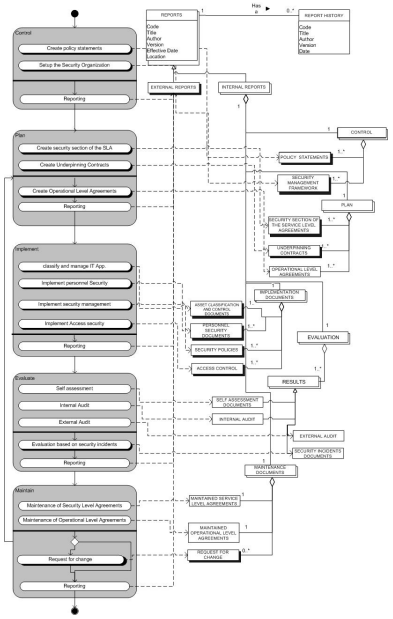

Figure 2.6.1: Process-data model Security Management process

Relations with other ITIL processes

The security Management Process, as stated in the introduction, has relations with almost all other ITIL-processes. These processes are:

- IT Customer Relationship Management
- Service Level Management
- Availability Management
- Capacity Management
- IT Service Continuity Management
- Configuration Management
- Release Management
- Incident Management & Service Desk
- Problem Management
- Change Management (ITSM)

Within these processes there are a couple of activities concerning security that have to take place. These activities are done as required. The concerning process and its process manager are responsible for these activities. However, the Security Management will give indications to the concerning process on how these (security specific) activities should be structured.

Example

Internal E-mail Policies.

The use of internal e-mail in an organization has a lot of security risks. So if an organization chooses to use e-mail as a means of communication, it is highly needed that the organization implements a well thought e-mail security plan/policies. In this example the ITIL security Management approach is used to implement e-mail policies in an organization.

First of the Security management team is formed and the guidelines, of how the process should be carried out, are formulated and made clear to all employees and provider concerned. These actions are carried out in the Control phase of the Security Management process.

The next step in to process to implement e-mail policies is the Planning. In the Plan phase of the process the policies are formulated. Besides the policies that are already written in the Service Level Agreements the policies that are specific for the e-mail security are formulated and added to the service level agreements. At the end of this phase the entire plan is formulated and is ready to be implemented.

The following phase in the process is the actual implementation of the e-mail policies. The implementation is done according to the plan which was formulated in the preceding phase (Plan phase).

After the actual implementation the e-mail policies will be evaluated. In order to evaluate the implemented policies the organization will perform;

The last phase is the maintenance phase. In the maintenance phase the implemented e-mail policies are maintained. The organization now knows which policies are properly implemented and are properly followed and, which policies need more work in order to help the security plan of the organization and, if there are new policies that have to be implemented. At the end of this process the Request for change are formulated (if needed) and the e-mail policies are properly maintained.

In order for the organization to keep its security plan up-to-date the organization will have to perform the security management process continuously. There is no end to this process an organization can always better its security.

References

Bon van, J. (2004). IT-Service management: een introductie op basis van ITIL. Van Haren Publishing

Cazemier, Jacques A.; Overbeek, Paul L.; Peters, Louk M. (2000). Security Management, Stationery Office.

Security management. (February 1, 2005). Retrieved from Microsoft Technet Web site: http://www.microsoft.com/technet/itsolutions/cits/mo/smf/mofsmsmf.mspx

Tse, D. (2005). Security in Modern Business: security assessment model for information security Practices. Hong Kong: University of Hong Kong.

External links

- Open Security Architecture [2]
- Microsoft Operations framework homepage [3]
- ISO/IEC 17799 website [4]
- The OGC website [5]
- IT Service Management Forum [6]
- The ITIL definition site [7]
- The ITIL Forum [8]
- ITIL wiki [9]
- Microsoft American ITIL [10]
- ITIL Security [11]

- Information Security Management maturity model [12]

References

[1] http://www.iso.org/iso/catalogue_detail?csnumber=42103
[2] http://www.opensecurityarchitecture.org
[3] http://www.microsoft.com/technet/itsolutions/cits/mo/mof/default.mspx
[4] http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html
[5] http://www.itil.co.uk
[6] http://www.itsmf.com
[7] http://www.itil.org.uk
[8] http://www.itilcommunity.com
[9] http://itil.technorealism.org
[10] http://www.govtech.net/magazine/channel_story.php/95672
[11] http://www.itil-service-management-shop.com/security.htm
[12] http://www.ism3.com

Article Sources and Contributors

ITIL security management *Source*: https://en.wikipedia.org/w/index.php?oldid=601437243 *Contributors*: Andrewman327, Ant, Aspects, Bejnar, Chris the speller, Conniecchang, Covington, EagleFan, Edward, HvL, J04n, Jlmata, Jncraton, John of Reading, Kuru, Mauls, Mgillett, Mjanulaitis, Mmairs, R'n'B, RHaworth, Royce, Saxbryn, Schoenjj, Siebrand, The Thing That Should Not Be, Vaceituno, Woohookitty, 27 anonymous edits

Image Sources, Licenses and Contributors

Image:Control Process model.jpg *Source*: https://en.wikipedia.org/w/index.php?title=File:Control_Process_model.jpg *License*: Creative Commons Attribution-Sharealike 2.5 *Contributors*: Bkell, Jlmata

Image:Control Data model.JPG *Source*: https://en.wikipedia.org/w/index.php?title=File:Control_Data_model.JPG *License*: Creative Commons Attribution-Sharealike 2.5 *Contributors*: Bkell, Jlmata

Image:Control Process data model.JPG *Source*: https://en.wikipedia.org/w/index.php?title=File:Control_Process_data_model.JPG *License*: Creative Commons Attribution-Sharealike 2.5 *Contributors*: Bkell, Jlmata

Image:Plan process data model.jpg *Source*: https://en.wikipedia.org/w/index.php?title=File:Plan_process_data_model.jpg *License*: Creative Commons Attribution-Sharealike 2.5 *Contributors*: Bkell, Jlmata

Image:Implementation process data model.jpg *Source*: https://en.wikipedia.org/w/index.php?title=File:Implementation_process_data_model.jpg *License*: Creative Commons Attribution-Sharealike 2.5 *Contributors*: Bkell, Jlmata, Where, 1 anonymous edits

Image:evaluation process data model.jpg *Source*: https://en.wikipedia.org/w/index.php?title=File:Evaluation_process_data_model.jpg *License*: Creative Commons Attribution-Sharealike 2.5 *Contributors*: Bkell, Jlmata

Image:Maintenance process data model.jpg *Source*: https://en.wikipedia.org/w/index.php?title=File:Maintenance_process_data_model.jpg *License*: Creative Commons Attribution-Sharealike 2.5 *Contributors*: Bkell, Jlmata

Image:Process data model security management.jpg *Source*: https://en.wikipedia.org/w/index.php?title=File:Process_data_model_security_management.jpg *License*: Creative Commons Attribution-Sharealike 2.5 *Contributors*: Bkell, Jlmata

License