Mapping ISO 27002 into Security Ontology

Ferran Alcázar
Vienna University of Technology
Barcelona, Spain
alcazar.ferran@gmail.com

Stefan Fenz
SBA Research and Vienna University of Technology
Vienna, Austria
sfenz@sba-research.org

ABSTRACT

In recent years, due to the increasingly interconnected environment, information is exposed to a growing number of threats and vulnerabilities. Therefore, it is especially important for an organization to have an efficient information security management system. Recently, it has been observed that organisations are looking for standards of best practice for guidance on how to manage their information security infrastructures. In this way, they can demonstrate that their information is adequately secured, and show to their customers and business partners that they can be trusted with protection of the important information. This document presents a methodology of mapping the ISO 27002 standard knowledge to the security ontology and it is intended for organisations that aim to maintain compliance with it.

Keywords: Ontological mapping, information security best-practice guidelines, security ontology, ISO27002.

1. INTRODUCTION

Information exists in many forms, it can be written or printed, stored or transmitted electronically, shown on videos, or spoken in a conversation. In all of these forms, the information asset should be appropriately protected. The information systems and networks of organizations are faced with a wide range of security threats like fraud, espionage, vandalism, fire or flood. In order for an organization to survive it is essential that they secure their information through implementation of a suitable set of controls, policies, procedures and software and hardware functions. All of these measures should be considered in a comprehensive approach and done in conjunction with other business management processes. The information security is something not to be considered in isolation but it should be considered in an early stage and as an important element in the overall development process. Aspects such as reliability, security and information privacy have moved from being mere matters of designers of information systems to becoming critical issues of vital importance for a business, organization and the society.

2. ONTOLOGIC ENGINIERING APPLIED ON THE INFORMATION SECURITY

According to Tom Gruber's definition an ontology is a formal specification of a shared conceptualization of a domain of interest. The ontology applied in computer science is a way to specify the meaning of content in a machine-understandable manner. Like medical students, who must learn medical ontology as a part of their education in order to prevent errors and improve quality of their work, professionals in information technology should also know the meanings and relationships of the terms that they handle, in order to share and agree with the basic concepts of the problem they are focusing on.

Security ontology provides a well-known basis to support the development of methods, processes and appropriate methodologies. IEEE editors point out in [1] the importance of ontologies and show a need within the security field for an ontology. A good ontology will help to organize and transmit knowledge, to check and report incidents effectively and share data and information through the organizations.

To sumarize, the application of the ontology in the security field contributes in the following ways [2]:

- Knowledge sharing and reuse for communication among people.
- Interoperability between software agents.
- Reusing domain knowledge.
- Making domain knowledge explicit.

3. ONTOLOGICAL STRUCTURE ANALYSIS

First step is to represent the overall design of the security ontology with textual, graphical and description logics representations. This ontological code was derived from best-practice guidelines and information security standards and it follows the OWL-DL (W3C Web Ontology Language) [3] to ensure that the concepts used and their relations represented are in a standardized and formal form.

The Figure 1 shows the overview of the concepts and relationships in the information security ontology. Each individual concept has a relationship with one or more of other concepts.

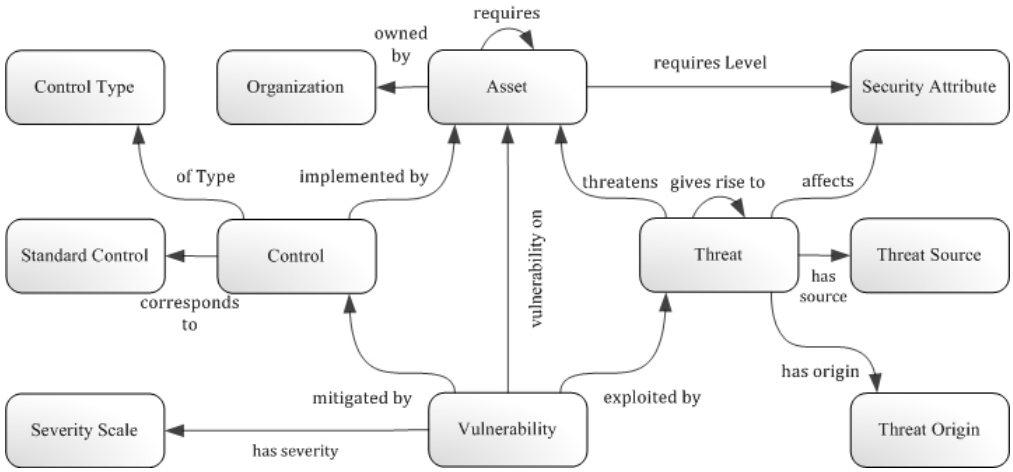


Figure 1. Overview of information security ontology concepts and relationships.

The central elements are threats, vulnerabilities, controls, and their implementations. As soon as a threat exploits a physical, technical, or administrative weakness, it gives rise to follow-upthreats, represents a potential danger to the organization's assets, and affects specific security attributes (e.g., confidentiality, integrity, and/or availability). We also use potential threat origins (human or natural origin) and sources (accidental or deliberate source) to describe each threat. Each vulnerability is assigned a severity value and the asset on which it could be exploited. Decision makers have to implement controls to mitigate identified vulnerability and to protect the respective assets through preventive, corrective, deterrent, recovery, or detective measures (control type) [4].

4. KNOWLEDGE BASE ANALYSIS

The International Standard ISO/IEC 27002 was prepared by Joint Technical Committee ISO/IEC JTC1, Information technology, Subcommittee SC 27, IT Security techniques. This International Standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined in this International Standard provide general guidance on the commonly accepted goals for information security management [5].

In Table 1 are listed de terms and definitions applied in the International Standard.

TERM	DEFINITION
Asset	Anything that has value to the organization. *[ISO/IEC 13335-1:2004]*
Control	Means of managing risk, including polices, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature.
Guideline	A description that clarifies what should be done and how, to achieve the objectives set out in policies. *[ISO/IEC 13335-1:2004]*
information processing facilities	Any information processing system, service o infrastructures, or the physical locations housing them.
Information security	Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved.
Information security event	It is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant. *[ISO/IEC TR 18044:2004]*
Information security incident	It is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. *[ISO/IEC TR 18044:2004]*
Policy	Overall intention and direction as formally expressed by management.
Risk	Combination of the probability of an event and its consequence. *[ISO Guide 73:2002]*
Risk analysis	Systematic use of information to identify sources and to estimate the risk. *[ISO Guide 73:2002]*
Risk evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk. *[ISO Guide 73:2002]*
Risk assessment	Overall process of risk analysis and risk evaluation. *[ISO Guide 73:2002]*
Risk management	Coordinated activities to direct and control an organization with regard to risk. *[ISO Guide 73:2002]*
Risk treatment	Process of selection and implementation of measures to modify risk. *[ISO Guide 73:2002]*
Third party	That person or body that is recognized as being independent of the parties involved, as concerns the issue in question. *[ISO Guide 2:1996]*
Threat	A potential cause of an unwanted incident, which may result in harm to a system or organization. *[ISO/IEC 13335-1:2004]*
Vulnerability	A weakness of an asset or group of assets that can be exploited by a threat. *[ISO/IEC 13335-1:2004]*

Table 1. ISO27002 concepts

The standard contains 11 security ***Clauses*** collectively containing a total of 39 main security ***Categories***. Each category contains a *control objective* and ***Guidelines*** with a *control statement* to achieve the objective. They also include an *implementation guidance*, which provides more detailed information to support the implementation of the control and meeting the control objective. In some cases, the implementation guidance is broken down into discrete steps, ***Guideline Steps***. The guideline ends with *other information* section that provides further information that may need to be considered, such legal considerations or references to other standards.

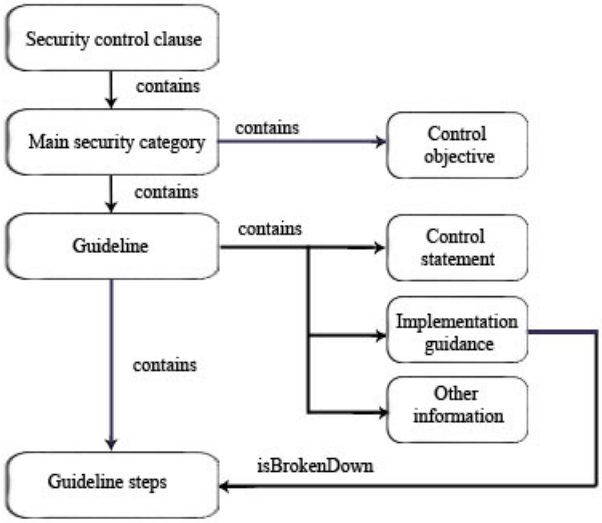


Figure 2. Structure of ISO27002

Figure 3 summarizes [6] the main sections of the standard. The order of clauses does not imply their importance. Each organization applying this standard should identify their clauses and the importance of them.

Figure 3. Summary of ISO27002 content.

There is no specified ontology made for this standard but ISO 27001 ontology [7,8] can be extended to get the ISO27002 ontology. The more significant modification is the *Guideline* addition, which is what really treats the standard.

Figure 4 illustrates the ontological mapping of the clause *"5.Security police"*. To enhance the readability only a short explanation is given in the control description and guideline steps fields.

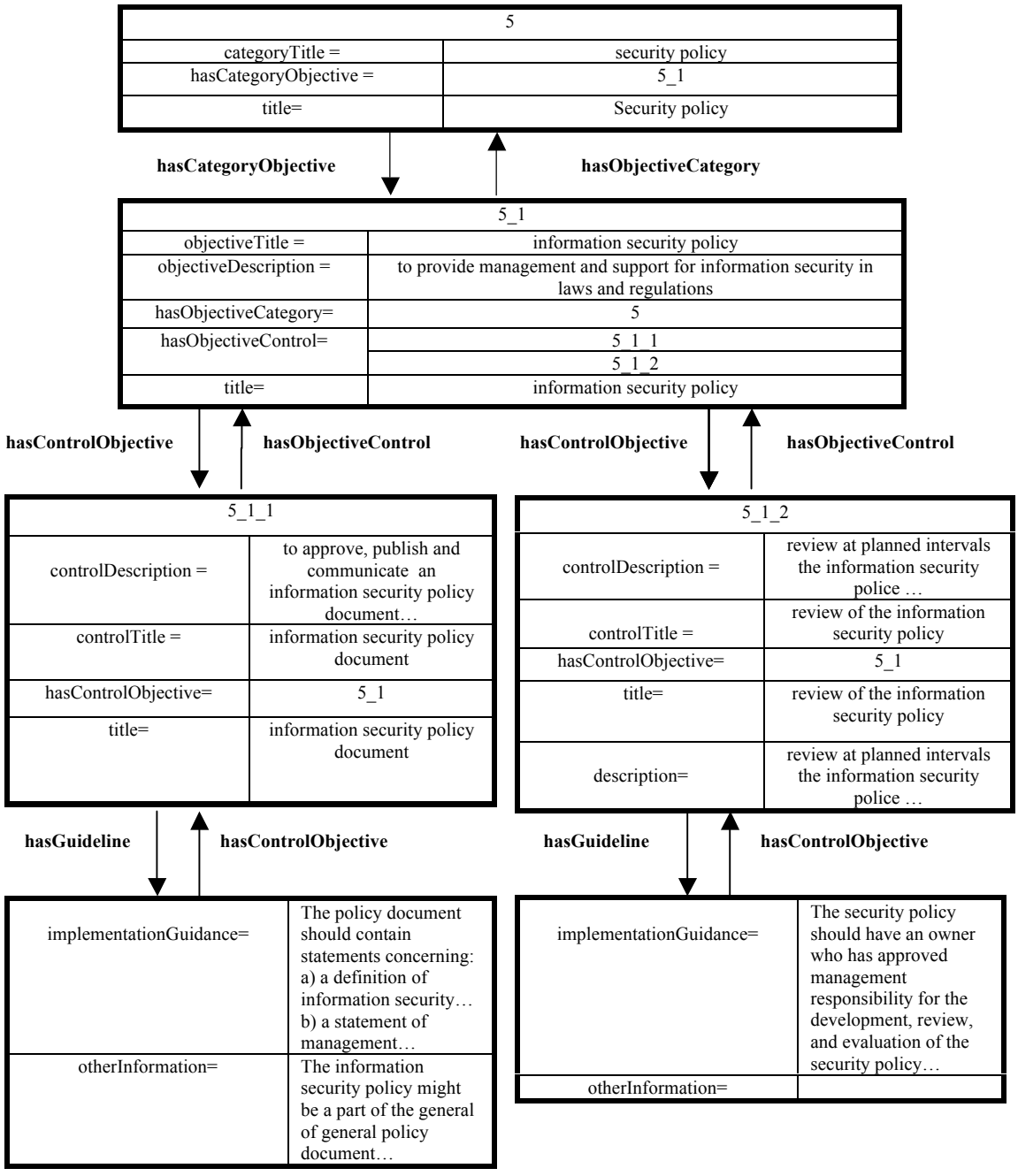


Figure 4. ISO27002 ontology.

5. MAPPING METHOD

To map the standard into the security ontology it is necessary to develop a customized method in order not to miss any security guidelines included. The following steps are:

1) ISO27002 structure analysis.

First, it is necessary to analyse and identify the structure of the ISO 27002. As mentioned before, the standard contains 11 security ***Clauses*** and 39 main security ***Categories.*** Each category contains ***Guidelines*** with a *control statement* to satisfy the *control objective.* It also contains an *implementation guidance*, which, in some cases, is broken down into ***Guideline Steps***. The guideline ends with *other information* section that provides further information such legal considerations or references to other standards.

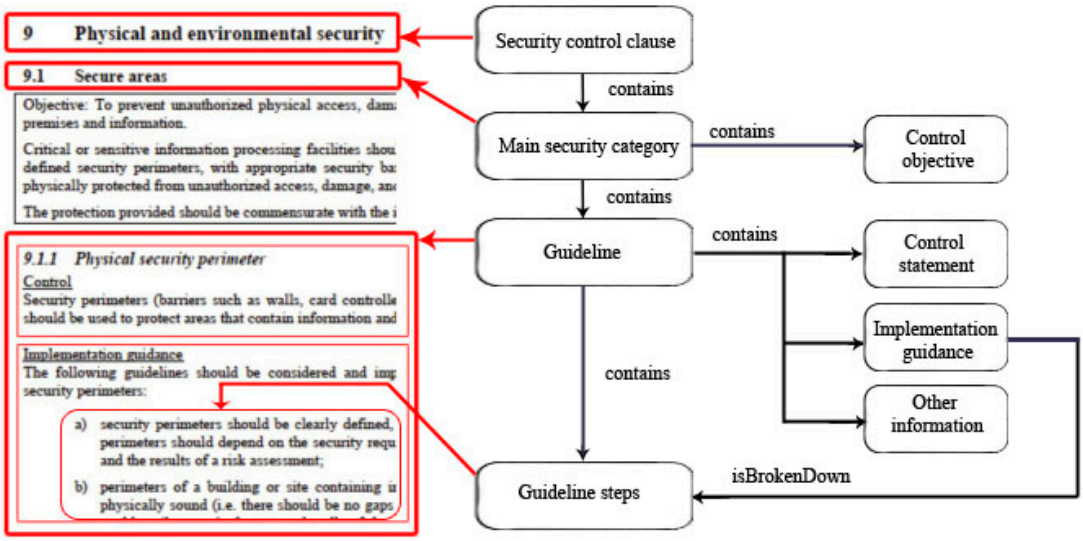


Figure 5. ISO27002 structure analysis.

The first conclusion obtained after analysing the standard, is that the mapping method will be focused on the control concept (security ontology top-level concept) and from this point, relations with the other concepts will be created.

2) Scanning analogies between both documents

Analysing security ontology and ISO 27002, it can be clearly observed that top-level concepts are the same. We can find the description of control, asset, vulnerability and threat defined in the same way, so all the mapping processes will be direct.

Each control can be directly extracted from the topic of the each guideline or in some cases, steps of the impletmentation guidance can be a control by themselves. The rest of top-level concepts can be deducted from the explanation of each guideline.

3) Including standard structure in the ontology

Next step is to include the standard structure (clause, category and guideline) in to the security ontology.

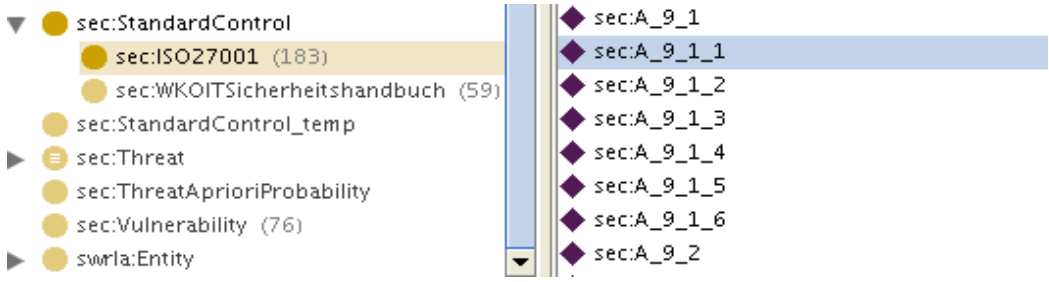


Figure 6. Including standard structure.

4) Mapping each standard control

The existing control concepts in the ontology and new added standard controls should be compared to identify analogies and to not to duplicate these concepts All the mapping information and details are included in the ***annex*** at the end of this document.

The following method has been used to map in the standard controls to the security ontology:

1. To analyze the existing controls and their descriptions.
2. To analyze the standard controls starting with the first control (5.1.1)
3. To decide if the standard control is needed to be mapped in one or more controls in accordance with its implementation guidance.
4. To compare and search for direct mapping of the existing controls .
5. To create a new security control in the ontology considering the description of the standard control.
6. To develop an accurate description and formal rules of the new control.

Standard controls guidelines are different among themselves. The method to map the control concept varies according to the standard control, and because of this it has been taken into account the following points:

- Some standard controls are grouped in a new security ontology control more general that include them. This control contains the specifications and the objectives of all of them. (e.g. *ComplianceControl*)

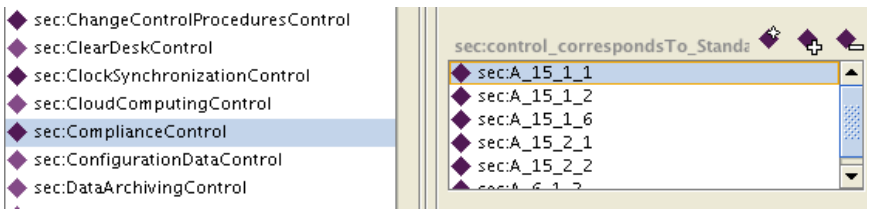


Figure 7. Control mapping.

- Some standard controls are mapped directly in a new or existing control.
    - *"10.10.6 Clock synchronization"* mapped to *ClockSynchronizationControl*
    - *"8.2.2 Information security awareness, education, and training"* mapped to *SecurityTrainingControl*

- The steps in the implementation guidance can be controls by themselves (e.g. *VisibleIdentificationControl*) or they can be just steps to be followed or advices to achieve the control objective defined in the guideline (e.g. *CablingSecurityControl*)

- In some cases the standard control is mapped in a "existing" control and it is also mapped in a "new" control more generic that covers some missed points. (*e.g. MediaDisposalControl* and *DataDisposalControl*)

5) Connecting vulnerabilities, threats and assets

Finally the rest of central elements is to be added to complete the mapping of the standard.

As it was showed before, each control mitigates one or more vulnerabilities, and each vulnerability has one or more threats that exploit it. Every vulnerability affects organizations assets, and the organization should apply the control exposed in the standard to mitigate it.

As in the case of control mapping, the relations will be made analyzing, if the top level concepts are already in the ontology or if it is necessary to create new ones. In some cases it is necessary to add new assets, such as policies or software, in the ontology to complete and satisfy the new rules of the concepts.

6. EXAMPLE

To explain the used method with more clarity *'CablingSecurityControl'*example will be showen:

StandardControl
◊ '9.2.3. Cabling security' • Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.
Asset
CablingSecurityPolicy ⊆ Policy
Vulnerability
◊ 'NoCablingSecurity'
Thread
◊ 'Fire (TopLevelThread) ◊ 'Flood'(LowLevelThread)

◊ 'ShortCircuit '(LowLevelThread) ◊ 'Vandalism' (LowLevelThread)
Control
◊ CablingSecurityControl CablingSecurityControlCompliantBuilding ⊆ Control

Figure 8. Mapping "9.2.3 Cabling security" control.

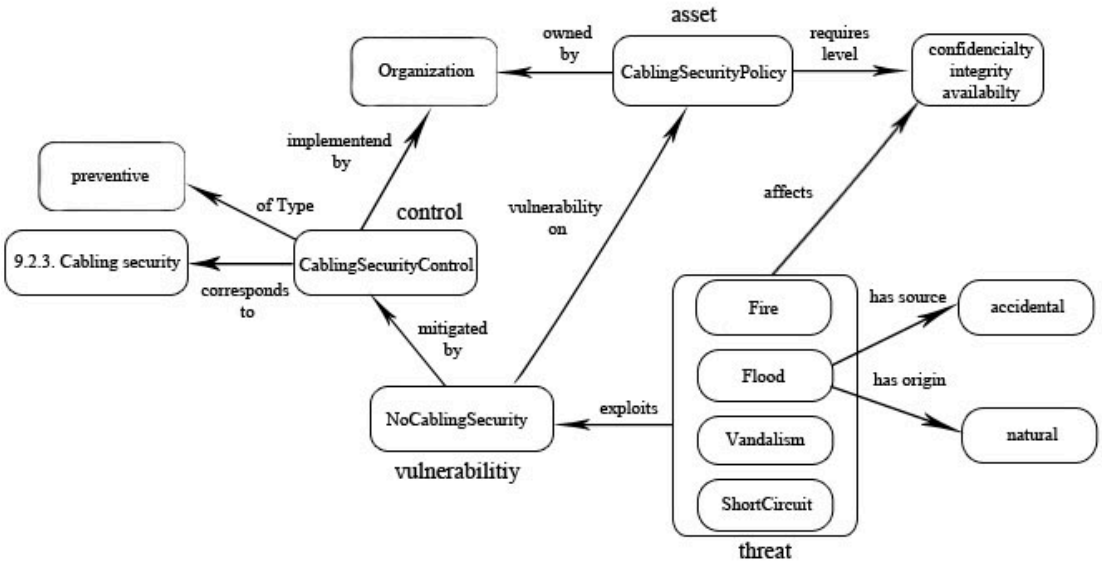


Figure 9. Mapping Schema

7. DIFFICULTIES IN THE MAPPING PROCESS

During the mapping process the following problems had to be solved to achieve the proposed goal:

ISO/IEC 27002 special standardization norm: It is necessary to take into account that ISO/IEC is not really a norm, it is a code of best practices recommendations and its structure complicates the mapping of some already existing concepts in the security ontology.

Identification of Existing Concepts in the Ontology: It is necessary to scan for analogies between both documents and to consider in detail if the found items correspond to their respective counterpart. After that, the mapping process can be direct or indirect.

Hide Concepts for Threats and Vulnerabilities: Although the concepts are explained and used in the standard, it is necessary to investigate each control to identify their different vulnerabilities and threats.

8. CONCLUSION

In today's world of information, where technology makes creation, distribution and manipulation of information easier, an appropriate IT security knowledge management is needed to ensure the correct flow of organizations' essential activities, often faced with security threats from a wide range of sources. It is necessary for an organization to identify vulnerabilities of their assets and establish appropriate controls to mitigate them. In this panorama of information security, there are many knowledge bases, and in this paper we proposed a method for mapping two of them. On one hand, there are information security standards and guidelines that aim to help organizations to implement security controls in order to protect organization's assets. On the other hand, there are security ontologies that facilitate sharing knowledge and reusing information between organizations. The developed method allows ISO 27002 to be transformed into OWL-code used by the security ontology. In this way we improve the existing security ontology with accepted information security knowledge. The limitations of the introduced method are: (i) there is an assumption that this method begins with the control concept, (ii) Subjectivity plays a significant role in regards to the selection of the controls. This mapping method can be useful for further similar guidelines that need to be mapped into the security ontology, contributing in this way to the professional security community.

9.REFERENCES

[1] Donner, M., Toward a Security Ontology. IEEE Security and Privacy, 2003
[2] M.Seidl. Introduction to Semantic Web. TU Wien
[3] W3C. OWL – web ontology language (February 2004)
[4] S.Fenz, A. Ekelhart. Formalizing Information Security Knowledge
[5] ISO/IEC 27002 International Standard
[6] ISO27002 Security forum *http://www.iso27001security.com/html/27002.html*
[7] ISO/IEC 27001 International Standard
[8] S.Fenz, E.Weippl. Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard
[9] S.Fenz, T.Pruckner, A.Manutscheri. Ontological Mapping of Information Security Best-Practice Guidelines

10. ANNEX: ISO/IEC 27002 CONTROL MAPPING

In this annex are described the new controls that complement the existing ones in the security ontology. Below each control its included:

- Description label (that will appear in the ontology)
- Extracts of each connected control of the standard.
- Ontology formal rules
- New additions (modifications and additions of the existing security ontology)
- Vulenrabilities
- Threads

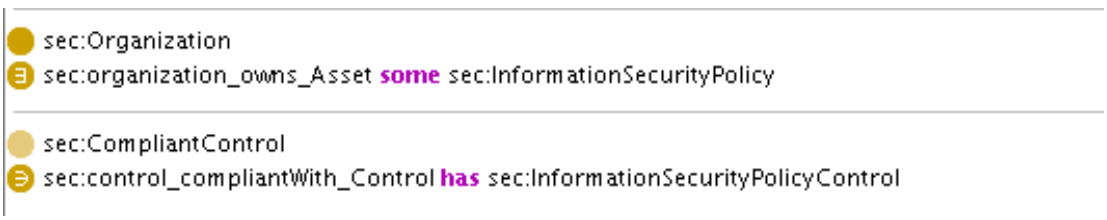
At the end of this document there is a complete mapping table.

- **InformationSecurityPolicyControl**

  Is there an Information Security Policy? Is it communicated to all employees and external parties? Is the use of unauthorized software included in the policy? Is the use of network and network services defined? Is it included an access control category in the policy? Is it included the use of cryptographic controls category?Is there a review of the Information Security Policy? Are there planned intervals to review it? Is it reviewed when significant changes occur?

  - An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties. *(Guideline 5.1.1)*
  - Establishing a formal policy prohibiting the use of unauthorized software. *(Implementation guidance 10.4.1.a)*
  - Establishing a formal policy to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium, indicating what protective measures should be taken. *(Implementation guidance 10.4.1.b)*
  - Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities. *(Guideline 10.8.1)*
  - Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems. *(Guideline 10.8.5)*
  - An access control policy should be established, documented, and reviewed based on business and security requirements for access. *(Guideline 11.1.1)*
  - A policy should be formulated concerning the use of networks and network services. *(Guideline 11.4.1)*
  - Restrictions to access should be based on individual business application requirements. The access control policy should also be consistent with the organizational access policy. *(Guideline 11.6.1)*
  - A policy on the use of cryptographic controls for protection of information should be developed and implemented. *(Guideline 12.3.1)*
  - The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness. *(Guideline 5.1.2)*

  Formal rules

New additions

sec:Asset > sec:IntangibleAsset > sec:Policy > sec:InformationSecurityPolicy
The policy document should contain statements concerning: a) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing; b) a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives; c) a framework for setting control objectives and controls, including the structure of risk assessment and risk management; d) a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including: 1) compliance with legislative, regulatory, and contractual requirements; 2) security education, training, and awareness requirements; 3) business continuity management; 4) consequences of information security policy violations; e) a definition of general and specific responsibilities for information security management, including reporting information security incidents; f) references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.

Vulnerability
◊ NoInformationSecurityPolicyControl

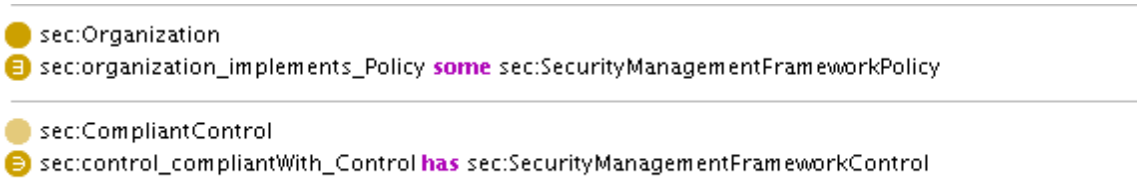
Threats
◊ AssetDamage
◊ AssetLoss
◊ DataDisclosure
◊ DataIntegrityLoss
◊ DataLoss
◊ FinalcialLoss
◊ ReputationLoss

- **SecurityManagementFrameworkControl**

Is there a commitment of the management to support actively the security? Is there a co-ordination of the security activities from different part of the organization?

- Management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities. *(Guideline 6.1.1)*
- Information security activities should be co-ordinated by representatives from different parts of the organization with relevant roles and job functions. *(Guideline 6.1.2)*

Formal rules



New additions

sec:Asset > sec:IntangibleAsset > sec:Policy > sec:SecurityManagementFrameworkPolicy
This policy should includ information about: • Management support of security information within the organization and demostrated commitment with security responsabilities. • Co-ordination of information security activities from different part of the organization. • Information security integral approach within the organization.

Vulnerability
◊ NoSecurityManagementFramework

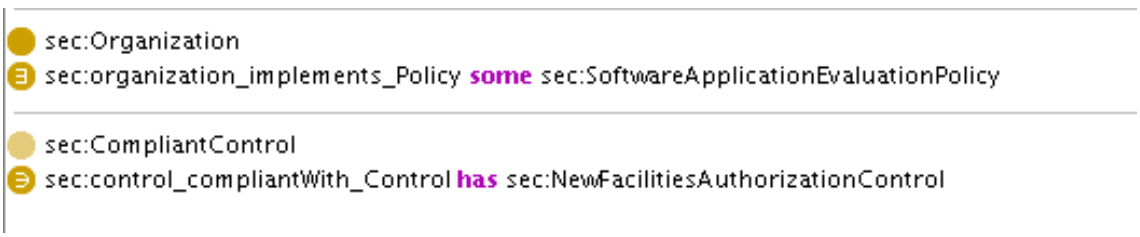
Threats
◊ UncoordinatedStaffMember *(New addition)*
◊ UntrainedStaffMember

- **NewFacilitiesAuthorizationControl**

Are the new facilities managed by authorization process? Are their hardware and software checked to ensure that they are compatible with other system components?Is there an acceptance criteria for new information systems and upgrades?

  - A management authorization process for new information processing facilities should be defined and implemented. *(Guideline 6.1.4)*
  - Acceptance criteria for new information systems, upgrades, and new versions should be established and suitable tests of the system(s) carried out during development and prior to acceptance. *(Guideline 10.3.2)*

Formal rules



Vulnerability
◊ NoNewFacilitiesAuthorization

Threats
◊ IncompatibleSystem *(New addition)*
◊ HardwareFailure

- **AppropriateContactsControl**

Does the organization maintain contacts with relevant authorities and special interest groups or security specialist?

  - Appropriate contacts with relevant authorities should be maintained. *(Guideline 6.1.6)*
  - Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained. *(Guideline 6.1.7)*

Formal rules

New additions

sec:Asset > sec:IntangibleAsset > sec:Policy > sec:AppropriateContactsPolicy
Policy should contain information about: • Procedures in place that specify when and by whom authorities (e.g. law enforcement, fire department, supervisory authorities) should be contacted. • How identified information security incidents should be reported in a timely manner if it is suspected that laws may have been broken. • Which contacts with special interest groups or other specialist security forums and professional associations are necessary to maintain for the organization. • Information sharing agreements with special interest groups.

Vulnerability
◊ NoAppropriateContacts

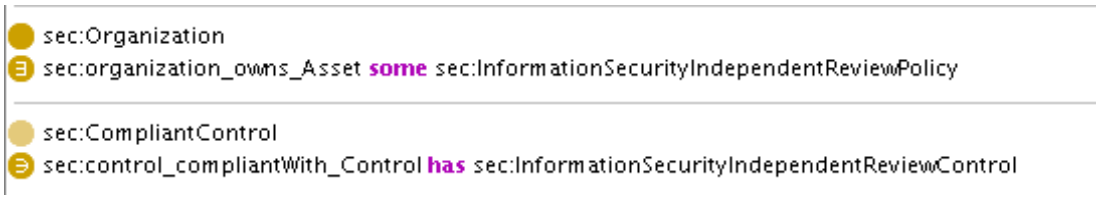
Threats
◊ LegalActions
◊ UntrainedStaffMember

- **InformationSecurityIndependentReviewControl**

Is the approach of the Information Security reviewed independently? Are there planned intervals to review it? Is it reviewed when significant changes occur?

  - The organization's approach to managing information security and its implementation (i.e. control objectives controls, policies, processes, and procedures for information security) should be reviewed independently at planned interval, or when significant changes to the security implementation occur. *(Guideline 6.1.8)*

Formal rules



New additions

sec:Asset > sec:IntangibleAsset > sec:Policy > sec:InformationSecurityIndependentReviewPolicy
This policy should contain: • Schedule of planned intervals to review the Information Security Policy. • Assessing opportunities for improvement and the need for changes to the approach to security, including the policy and control objectives • Reports of the independent review results.

Vulnerability
◊ NoInformationSecurityIndependentReview

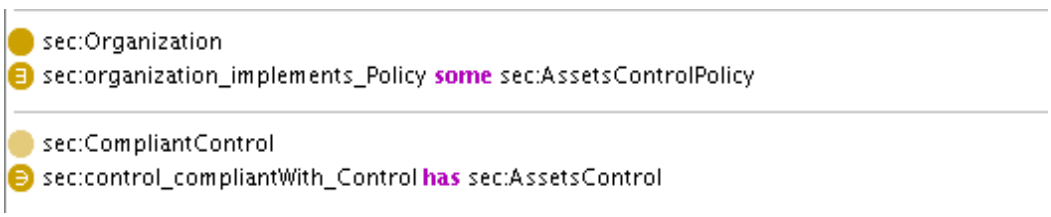
Threats
◊ UnawaredStaffMember *(New addition)*
◊ LegalActions

- **AssetsControl**

Are the important assets identified in an inventory? Is the inventory maintained? Are the information processing facilities assets owned by a designed part of the organization? Are rules for acceptable use of assets identified, documented and implemented?

  - All assets should be clearly identified and an inventory of all important assets drawn up and maintained. *(Guideline 7.1.1)*
  - All information and assets associated with information processing facilities should be owned by a designated part of the organization. *(Guideline 7.1.2)*
  - Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented. *(Guideline 7.1.3)*
  - A current and complete inventory of assets (see 7.1) is a prerequisite for effective technical vulnerability management. Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment (e.g. what software is installed on what systems), and the person(s) within the organization responsible for the software. *(Guideline 12.6.1)*

Formal rules



New additions

sec:Asset > sec:IntangibleAsset > sec:Policy > sec:AssetsControlPolicy
This policy should contain: • List of all assets and documentation about their importance. • Include for each asset: type of asset, format, location, backup information, license information and a business value. • Information classification and ownership of each asset. • Rules for the acceptable use of information and assets associates with information processing facilities

Vulnerability
◊ NoAssetsControl

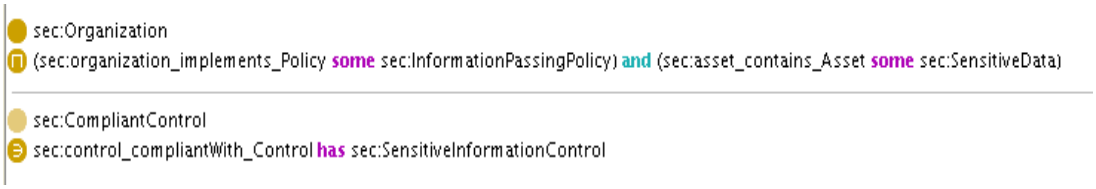
Threats
◊ Theft
◊ AssetLoss
◊ DataLoss

- **SensitiveInformationControl**

Is the sensitive information classified properly? Has the output sensitive information an appropriate classification label? Are there obvious signs to identify the presence of information processing facilities? Is the system documentation protected and stored securely? Is the information exposed in the public network properly protected?

  - Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization. *(Guideline 7.2.1)*
  - Output from systems containing information that is classified as being sensitive or critical should carry an appropriate classification label (in the output). The labelling should reflect the classification according to the rules established in 7.2.1. Items for consideration include printed reports, screen displays, recorded media (e.g. tapes, disks, CDs), Electronic messages, and file transfers. *(Guideline 7.2.2)*
  - All employees, contractors and third party users should return all of the organization's assets in their possession upon termination of their employment, contract or agreement. *(Guideline 8.3.2)*
  - Where applicable, buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities. *(Implementation guidance 9.1.3.c)*
  - Directories and internal telephone books identifying locations of sensitive information processing facilities should not be readily accessible by the public. *(Implementation guidance 9.1.3.d)*
  - Protection of spooled data awaiting output to a level consistent with its sensitivity. *(Implementation guidance 10.7.3.e)*
  - System documentation should be stored securely. *(Implementation guidance 10.7.4.a)*
  - The access list for system documentation should be kept to a minimum and authorized by the application owner; *(Implementation guidance 10.7.4.b)*
  - System documentation held on a public network, or supplied via a public network, should be appropriately protected. *(Implementation guidance 10.7.4.c)*
  - The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification. *(Guidance 10.9.3)*

Formal rules



New additions

SecAsset > sec:IntangibleAsset > sec:Policy > sec:InformationPassingPolicy
(addition of existing policy information) • Definiton of the controls to classify and handle sensitive information. In this controls have to be included input, output and public information. • Definition of the control to protect information held on public network or supplied via public network.

Vulnerability
◊ NoSensitiveInformationControl

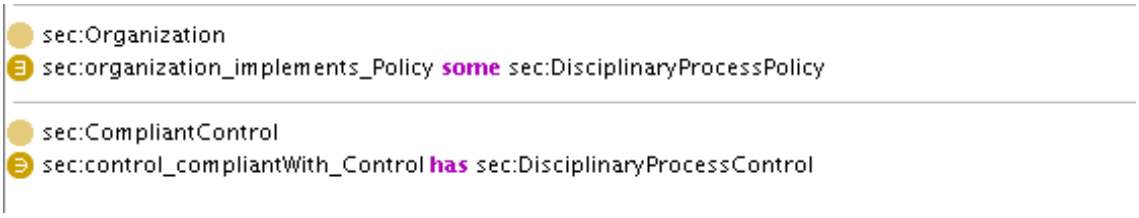
Threats
◊ DumpsterDiving
◊ IndustrialEspionage
◊ Sabotage
◊ DataDisclosure

- **DisciplinaryProcessControl**

Is there a disciplinary process for employees who have committed a security breach?

- There should be a formal disciplinary process for employees who have committed a security breach. *(Guideline 8.2.3)*
- Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal) evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). *(Guideline 13.2.3)*

Formal rules



New additions

sec:Asset > sec:IntangibleAsset > sec:Policy > sec:DisciplinaryProcessPolicy
The formal disciplinary process should ensure correct and fair treatment for employees who are suspected of committing breaches of security. The formal disciplinary process should provide for a graduated response that takes into consideration factors such as the nature and gravity of the breach and its impact on business, whether or not this is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required. In serious cases of misconduct the process should allow for instant removal of duties, access rights and privileges, and for immediate escorting out of the site, if necessary.

The disciplinary process should not be commenced without prior verification that a security breach has occurred.

Vulnerability
◊ NoDisciplinaryProcess

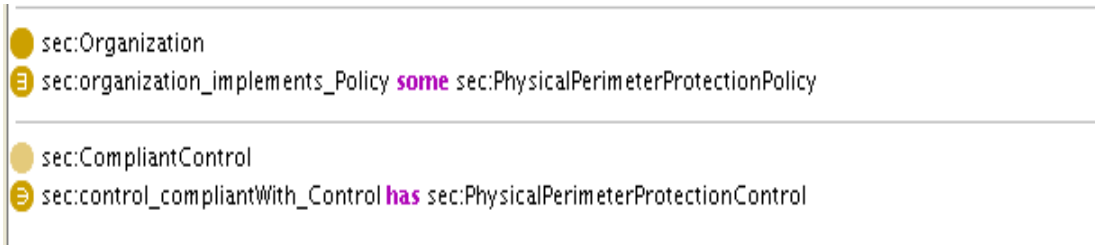
Threats
◊ EmployeeMisconduct

- **PhysicalPerimeterProtectionControl**

Are the security perimeters clearly defined? Are the important perimeters physically sound? Are the external wall made of a solid construction? Are the doors suitably protected against unauthorized access? Are the doors and windows locked?

- Security perimeters should be clearly defined, and the sitting and strength of each of the perimeters should depend on the security requirements of the assets within the perimeter and the results of a risk assessment. *(Implementation guidance 9.1.1.a)*
- Perimeters of a building or site containing information processing facilities should be physically sound (i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur); the external walls of the site should be of solid construction and all external doors should be suitably protected against unauthorized access with control mechanisms, e.g. bars, alarms, locks etc; doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level. *(Implementation guidance 9.1.1.b)*

Formal rules



New additions

sec:Asset > sec:IntangibleAsset > sec:Policy > sec:PhysicalPerimeterProtectionPolicy
This policy should include: • Clear definition of security perimeters. • Information about physical barriers to protect from unauthorized access, damage, and interfernece. • Which sensitive information processing facilities should be housed in secure areas. • Information about intruder detection systems. • Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster. • Physical protection and guidelines for working in secure areas.

Vulnerability
◊ NoPhysicalPerimeterProtectionPolicy

Threats
◊ Theft

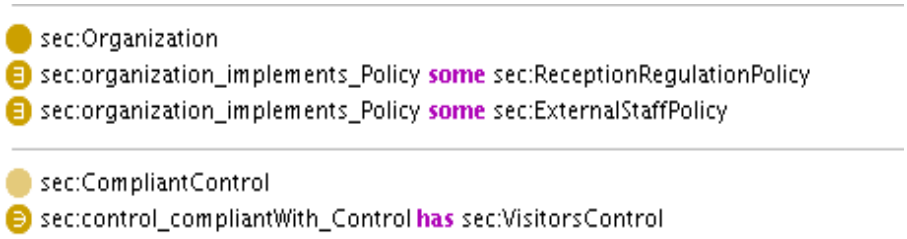
◊ Sabotage
◊ Vandalism

- **VisitorsControl**

Is the access of the visitors supervised? Are the date and time of entry and departure recorded?

- The date and time of entry and departure of visitors should be recorded, and all visitors should be supervised unless their access has been previously approved; they should only be granted access for specific, authorized purposes and should be issued with instructions on the security requirements of the area and on emergency procedures. *(Implementation guidance 9.1.2.a)*

Formal rules



Vulnerability
◊ NoVisitorsControl

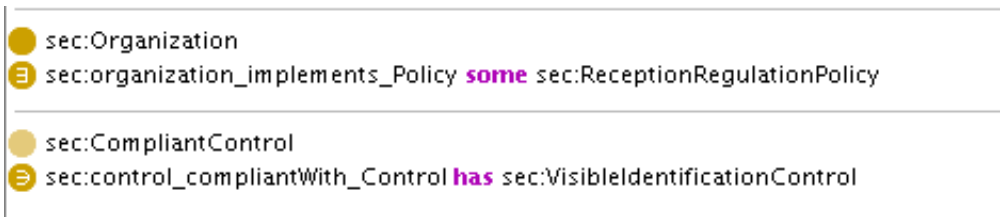
Threats
◊ BreakIn
◊ Theft
◊ UnauthorizedPhysycalAccess

- **VisibleIdentificationControl**

Is there a visible identification for all employees, contractors, third party users and visitors?

- All employees, contractors and third party users and all visitors should be required to wear some form of visible identification and should immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification. *(Implementation guidance 9.1.2.c)*

Formal rules



Vulnerability
◊ NoVisitorsControl

Threats
◊ BreakIn
◊ Theft

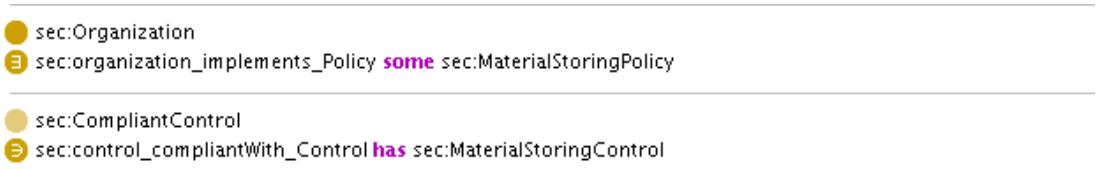
◊ UnauthorizedPhysycalAccess

- ## MaterialStoringControl

Are the combustible and dangerous materials stored at a safe distance from a secure area? Are bulk supplies stored within a secure area? Is the back-up media stored in a safe location?

- Hazardous or combustible materials should be stored at a safe distance from a secure area; Bulk supplies such as stationery should not be stored within a secure area; *(Implementation guidance 9.1.4.a)*
- Fallback equipment and back-up media should be sited at a safe distance to avoid damage from a disaster affecting the main site. *(Implementation guidance 9.1.4.b)*

Formal rules



New additions

sec:Asset > sec:IntangibleAsset > sec:Policy > sec:MaterialStoringPolicy
Policy should contain information about: • Which hazardous or combustible materials should be stored at a safe distance from a secure area. • Where bulk supplies such a stationery should not be stored within a secure area. • Where fallback equoment and back-up media should be sited to be at a safe distance to avoid damage from a disaster affecting the main site.

Vulnerability
◊ NoMaterialStoring

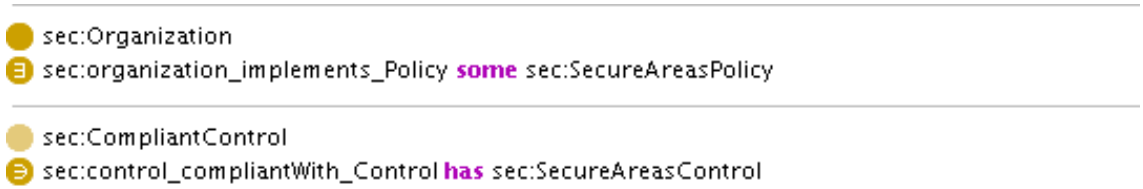
Threats
◊ DumpsterDiving
◊ Fire

- ## SecureAreasControl

Is there physical protection and guidelines for working in secure areas?

- Personnel should only be aware of the existence of, or activities within, a secure area on a need to know basis. *(Implementation guidance 9.1.5.a)*
- Unsupervised working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities. *(Implementation guidance 9.1.5.b)*
- Vacant secure areas should be physically locked and periodically checked. *(Implementation guidance 9.1.5.c)*
- Photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed, unless authorized. *(Implementation guidance 9.1.5.d)*

Formal Rules



New additions

secAsset > sec:IntangibleAsset > sec:Policy > sec:SecureAreasPolicy
This policy should include the following statements: - personnel should only be aware of the existence of, or activities within, a secure area on a need to know basis; - unsupervised working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities; - vacant secure areas should be physically locked and periodically checked; -photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed, unless authorized;

Vulnerability
◊ NoSecureAreasControl

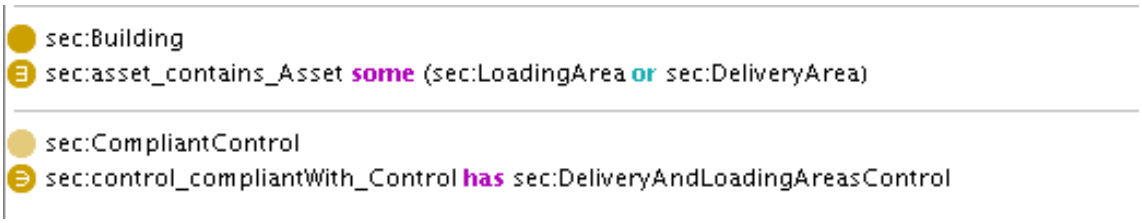
Threats
◊ IndustrialEspionage
◊ Theft

- **DeliveryAndLoadingAreasControl**

Is the access to delivery and loading areas restricted to the identified and authorized personnel?

  - Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. *(Implementation guidance 9.1.6)*

Formal rules



New additions

sec:Asset > sec:TangibleAsset > sec:ImmovableAsset > sec: Section > sec:LoadingArea
sec:Asset > sec:TangibleAsset > sec:ImmovableAsset > sec: Section > sec: DeliveringArea

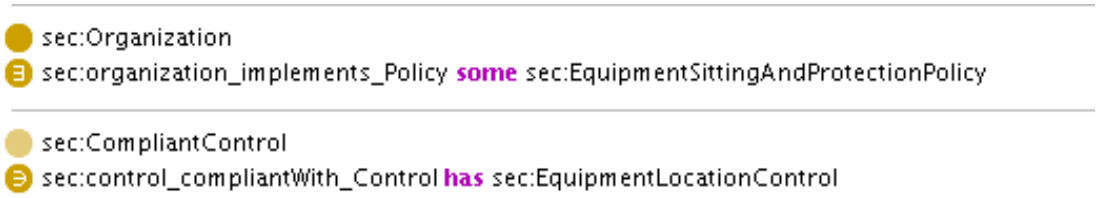
Vulnerability
◊ NoDeliveryAndLoadingAreas
Threats
◊ UnauthorizedPhysicalAccess

- **EquipmentLocationControl**

Is the equipment sited minimizing unnecessary access to work areas? Are the information processing facilities positioned in order to reduce the risk of unauthorized access? Are special items isolated?

  - Equipment should be sited to minimize unnecessary access into work areas. *(Implementation guidance 9.2.1.a)*
  - Information processing facilities handling sensitive data should be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorized persons during their use, and storage facilities secured to avoid unauthorized access. *(Implementation guidance 9.2.1.b)*
  - Items requiring special protection should be isolated to reduce the general level of protection required; *(Implementation guidance 9.2.1.c)*

Formal Rules



New additions

sec:Asset > sec:IntangibleAsset > sec:Policy > sec:EquipmentSittingAndProtectionPolicy
Policy should contain information about: • The situation of the equipment to minimize unnecessary acces into work areas. Furthermore, information processing facilities handling sensitive data should be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorizedpersons during their use, and storage facilities secured to avoid unauthorized access; • Identificaiton of items that require special protection in order to be isolated to reduce the general level ofprotection required. • Controls that should be adopted to minimize the risk of potential physical threats, e.g. theft,fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects,electrical supply interference, communications interference, electromagnetic radiation,and vandalism;

Vulnerability
◊ NoEquipmentLocationControl

Threats
◊ UnauthorizedPhysicalAccess
◊ Fire
◊ Flood

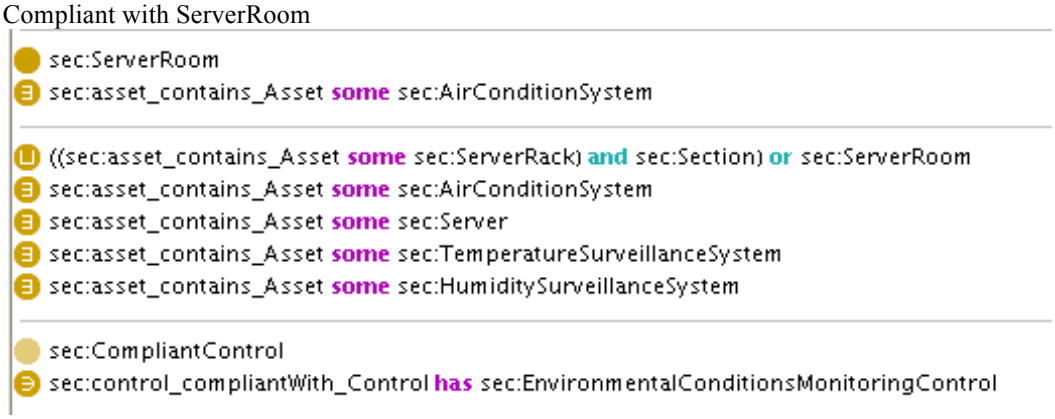
- **EnvironmentalConditionsMonitoringControl**

  Are environmental conditions monitored?

  - Environmental conditions, such as temperature and humidity, should be monitored for conditions, which could adversely affect the operation of information processing facilities *(Implementation guidance 9.2.1.f)*

  Formal rules

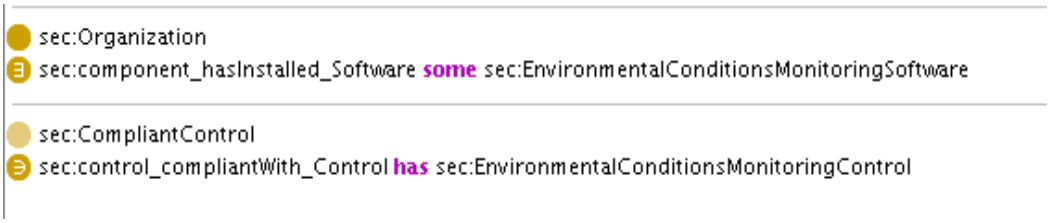
  Compliant with ServerRoom

  New additions

sec:Asset > sec:TangibleAsset > sec:MovableAsset > sec:HumiditySurveillanceSystem

  Compliant Organization

  New additions

sec:Asset > sec:IntangibleAsset > sec:Software > sec:EnvironmentalConditionsMonitoringSoftware
This software monitores environmental conditions, such as temperature and humidity.

  Vulnerability
  ◊ NoEnvironmentalConditionsMonitoring

  Threats
  ◊ InadmissableTemperatureAndHumidity

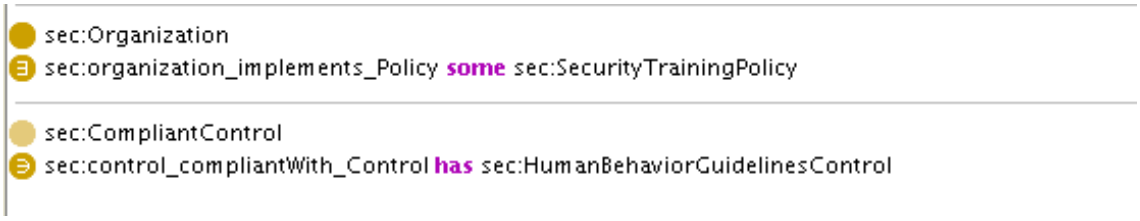
- **HumanBehaviorGuidelinesControl**

  Are guidelines established for human behaviour in the proximity to information processing facilities?

  - Guidelines for eating, drinking, and smoking in proximity to information processing

facilities should be established. *(Implementation guidance 9.2.1.e)*

Formal rules



New additions

SecAsset > sec:IntangibleAsset > sec:Policy > sec:SecurityTrainingPolicy
(addition of the existing policy information) Behaviour guidelines for eating, drinking and smoking in proximity to information processing facilities.

Vulnerability
◊ NoHumanBehaviorGuidelines

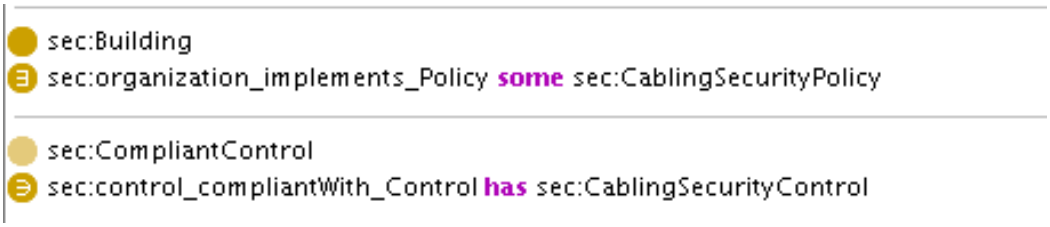
Threats
◊ EmployeesMisconduct

- **CablingSecurityControl**

Is the cabling protected for interception or damage? Is the cabling and patch panel clearly identifiable and properly marked?

- Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage. *(Guideline 9.2.3)*.

Formal rules



New additions

SecAsset > sec:IntangibleAsset > sec:Policy > sec:CablingSecurityPolicy
The following guidelines for cabling security should be considered: a) power and telecommunications lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection; b) network cabling should be protected from unauthorized interception or damage, for example by using a conduit or by avoiding routes through public areas; c) power cables should be segregated from communications cables to prevent interference; d) clearly identifiable cable and equipment markings should be used to minimise handling errors, such as accidentally patching of wrong network cables;

e) a documented patch list should be used to reduce the possibility of errors;
f) for sensitive or critical systems further controls to consider include:
1) installation of armoured conduit and locked rooms or boxes at inspection and termination points;
2) use of alternative routings and/or transmission media providing appropriate security;
3) use of fibre optic cabling;
4) use of electromagnetic shielding to protect the cables;
5) initiation of technical sweeps and physical inspections for unauthorized devices being
attached to the cables;
6) controlled access to patch panels and cable rooms.

Vulnerability
◊ NoCablingSecurity

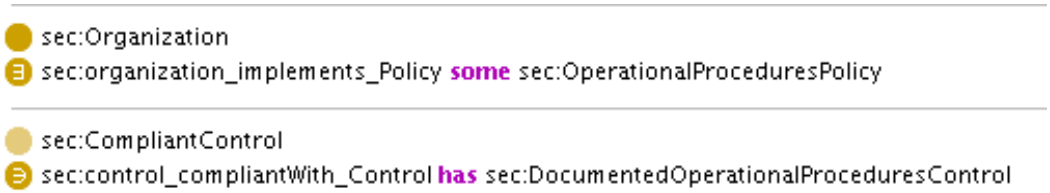
Threats
◊ Flood
◊ Fire
◊ Vandalism
◊ ShortCircuit

- **DocumentedOperationalProceduresControl**

Are the operational procedures documented and maintained? Are available to the users who need them?

- Operating procedures should be documented, maintained, and made available to all users who need them. *(Guideline 10.1.1)*

Formal rules



New addition

SecAsset > sec:IntangibleAsset > sec:Policy > sec:OperationalProceduresPolicy

This policy should include information about:

- How to ensure the correct and secure operation of information processing facilities.
- Responsibilities and procedures for the management and operation of all information processing facilities that should be established. This includes the development of appropriate operating procedures.
- Segregation of duties that should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

Vulnerability
◊ NonDocumentedOperationalProcedures

Threats
◊ ServiceMalfuction

- **ThirdPartyServiceManagementControl**

Is the third party service delivery agreement implemented, operated and maintained by the third party? Are the services, reports and records provided by the third party regularly monitored and reviewed? Are the changes of their services properly managed?

  - It should be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party. *(Guideline 10.2.1)*
  - The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly. *(Guideline 10.2.2)*
  - Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks. *(Guideline 10.2.3)*

Formal rules

Vulnerability
◊ NoThirdPartyServiceManagement

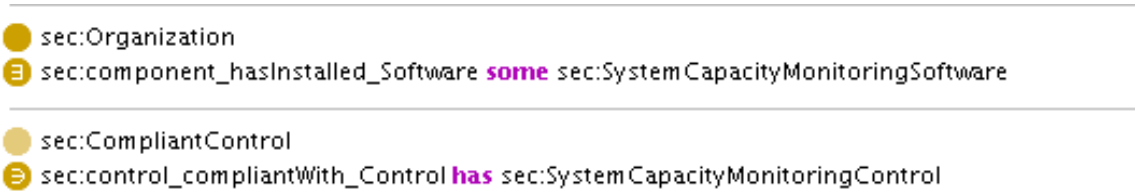
Threats
◊ DataDisclosure
◊ LegalAction
◊ UncontrolledThirdPartyService

- **SystemCapacityMonitoringControl**

Are the resources monitored? Are projections of future capacity requirements made?

  - The use of resources should be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance. *(Guideline 10.3.1)*

Formal rules



New additions

sec:Asset > sec:IntangibleAsset > sec:Software > sec:SystemCapacityMonitoringSoftware

Vulnerability
◊ NoSystemCapacityMonitoring

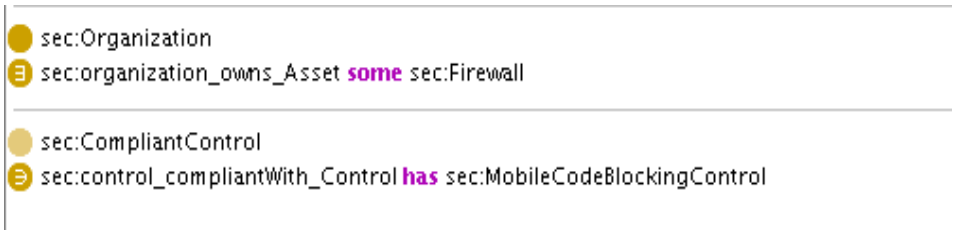
Threats
◊ ProductivityDecrease
◊ ServiceMalfunction

- **MobileCodeBlockingControl**

Is the use and reception of mobile code blocked?

  - Blocking any use of mobile code. *(Implementation guidance 10.4.2.b)*
  - Blocking receipt of mobile code. *(Implementation guidance 10.4.2.c)*

Formal rules



Vulnerability
◊ NoMobileCodeBlocking

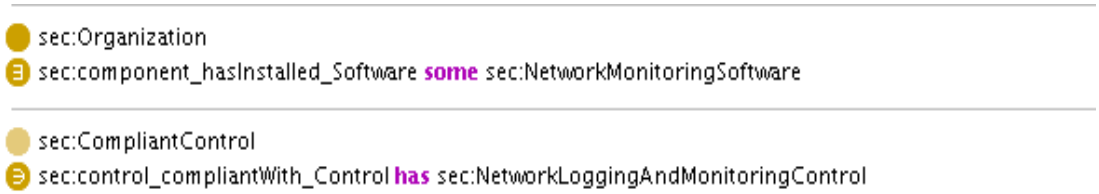
Threats
◊ VirusAndMalware

- **NetworkLoggingAndMonitoringControl**

Is there a logging and monitoring control?

  - Appropriate logging and monitoring should be applied to enable recording of security relevant actions. *(Implementation guidance 10.6.1.d)*

Formal rules



New rules

sec:Asset > sec:IntangibleAsset > sec:Software > sec:NetworkMonitoringSoftware

Vulnerability
◊ NoNetworkLoggingAndMonitoring

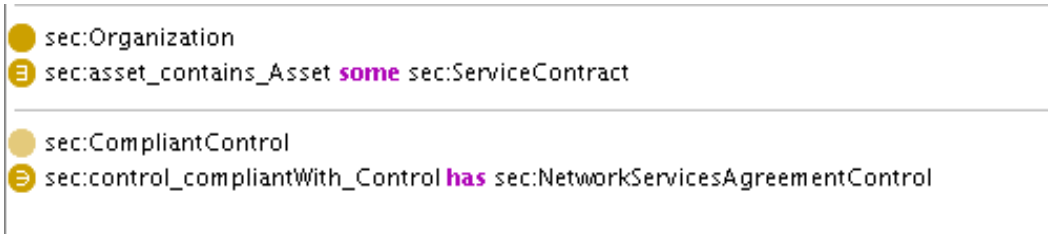
Threats
◊ NetworkAttack
◊ NetworkOutage

- ## NetworkServicesAgreementControl

Are the security features, services levels, and management requirements of all network services included in a services network agreement?

  - Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or outsourced. *(Guideline 10.6.2)*

Formal rules



Vulnerability
◊ InsufficientServiceLevelAgreement

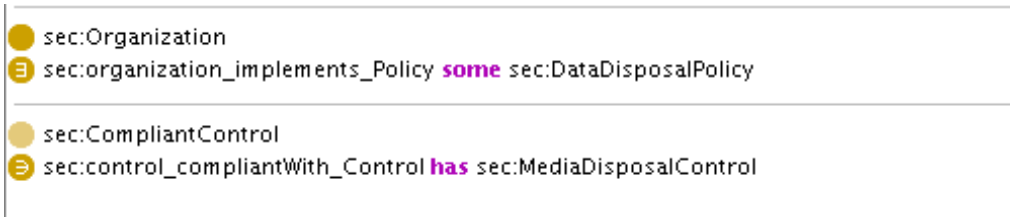
Threats
◊ LegalAction

- ## MediaDisposalControl

Are there formal procedures for the secure disposal of media?

  - Media should be disposed of securely and safely when no longer required, using formal procedures. Formal procedures for the secure disposal of media should minimize the risk of sensitive information leakage to unauthorised persons. The procedures for secure disposal of media containing sensitive information should be commensurate with the sensitivity of that information. *(Guideline 10.7.2)*

Formal rules



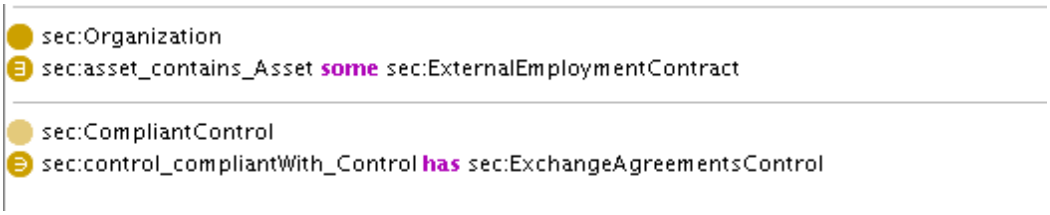
Vulnerability
◊ ImproperMediaDisposal

Threats
◊ DumpsterDiving

- **ExchangeAgreementsControl**

Are there agreements for the exchange of information and software between organization and external parties?

- Agreements should be established for the exchange of information and software between the organization and external parties. *(Guideline 10.8.2)*



Vulnerability
◊ NoExchangeAgreements

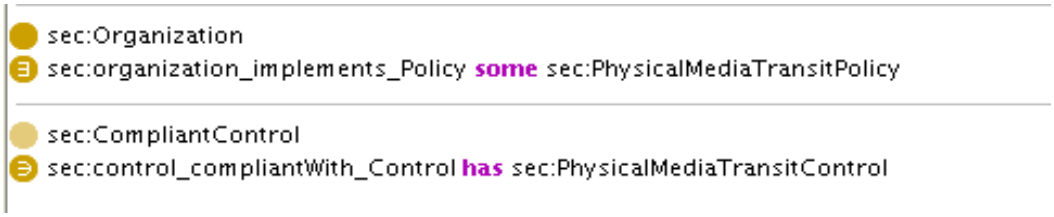
Threats
◊ LegalAction

- **PhysicalMediaTransitControl**

Is the media containing information that is being transported properly protected?

- Media containing information should be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries. *(Guideline 10.8.3)*

Formal rules



New addition

SecAsset > sec:IntangibleAsset > sec:Policy > sec:PhysicalMediaTransitPolicy
The following guidelines should be considered to protect information media being transported between sites: a) reliable transport or couriers should be used; b) a list of authorized couriers should be agreed with management; c) procedures to check the identification of couriers should be developed; d) packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications (e.g. for software), for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields; e) controls should be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification; examples include: 1) use of locked containers; 2) delivery by hand;

3) tamper-evident packaging (which reveals any attempt to gain access);
4) in exceptional cases, splitting of the consignment into more than one delivery and dispatch by different routes.

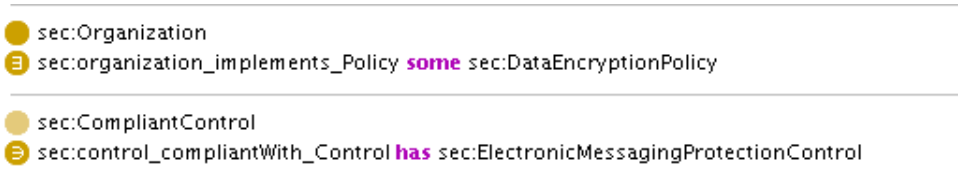
Vulnerability
◊ NoPhysicalMediaTransitControl
Threats
◊ AssetLoss
◊ AssetDamage

- **ElectronicMessagingProtectionControl**

Is the information involved in electronic messaging appropriately protected?

  - Information involved in electronic messaging should be appropriately protected. *(Guideline 10.9.1)*

Formal rules



Vulnerability
◊ NoElectronicMessagingAndComerceServiceProtection

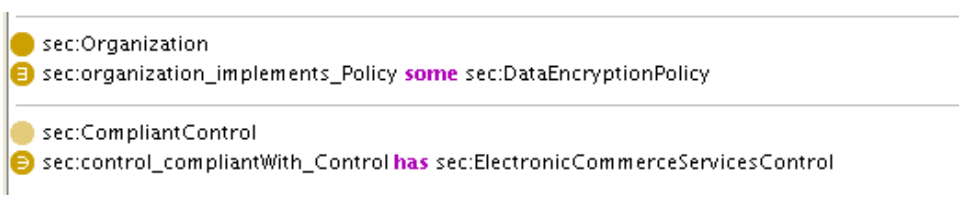
Threats
◊ DataLoss
◊ DataIntegrityLoss
◊ DataDisclosure

- **ElectronicCommerceServicesControl**

Is the electronic commerce information protected against fraud, unauthorized disclosure or modification? Are the on-line transactions protected to prevent incomplete transmission, message alteration, mis-routing, message duplication or replay?

  - Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification. *(Guideline 10.9.1)*
  - Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. *(Guideline 10.9.2)*

Formal rules



Vulnerability
◊ NoElectronicMessagingAndComerceServiceProtection

Threats
◊ DataLoss
◊ DataIntegrityLoss
◊ DataDisclosure

- ## AuditLoggingAndMonitoringControl

Is there a system of logs that shows the users activities, exceptions and security events? Are there procedures for monitoring the use of information processing facilities? Are the monitored results reviewed regularly? Are the computer systems monitoring the resource usage? Is there a review of fault logs? Is there a review of corrective measures to ensure that controls have not been compromised?

- Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring. *(Guideline 10.10.1)*
- Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly. *(Guideline 10.10.2)*
- Regular monitoring of personnel and system activities, where permitted under existing legislation or regulation, to avoid information leakage. *(Implementation guidance 12.5.4.d)*
- Monitoring resource usage in computer systems. *(Implementation guidance 12.5.4.e)*
- Faults should be logged, analysed, and appropriate action taken. *(Guideline 10.10.5)*

Formal rules

New additions

sec:Asset > sec:IntangibleAsset > sec:Software > sec:ActivitiesMonitoringSoftware
Software that monitors user's activities in the computers and networks.

SecAsset > sec:IntangibleAsset > sec:Policy > sec:AuditLoggingAndMonitoringPolicy
This policy should contain information about: • Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring. • Procedures for monitoring use of information processing facilities that should be established and the results of the monitoring activities reviewed regularly. • Regular monitoring of personnel and system activities, where permitted under existing legislation or regulation, to avoid information leakage. • Monitoring resource usage in computer systems. • Definition of faults that should be logged, analysed, and appropriate action taken.

Vulnerability
◊ NoAuditLoggingAndMonitoring

Threats

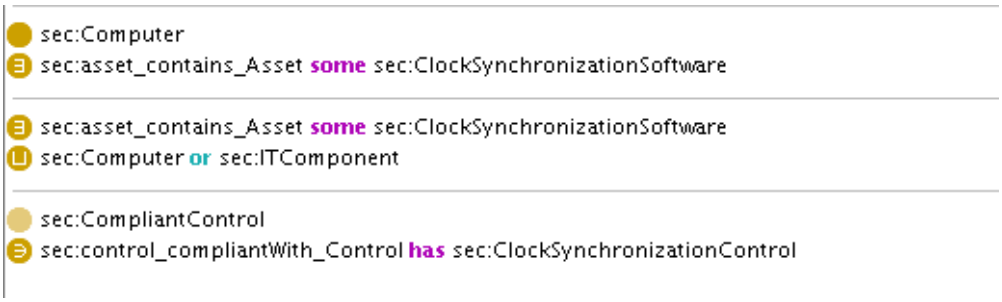
◊ UnauthorizedUseOfITSystems
◊ IndustrialEspionage

- ## ClockSynchronizationControl

Are the clocks of information processing systems synchronized?

  - The clocks of all relevant information processing systems within an organization or security domain should be synchronized with an agreed accurate time source. *(Guideline 10.10.6)*

Formal rules



New additions

sec:Asset > sec:IntangibleAsset > sec:Software > sec:ClockSynchronizationSoftware

Vulnerability
◊ NoClockSynchronization

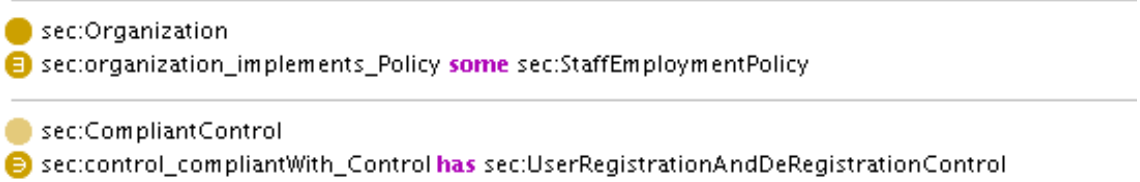
Threats
◊ ServiceMalfunction

- ## UserRegistrationAndDeRegistrationControl

Is there a formal procedure for user registration and de-registration? Is there a unique user ID? Are the groups ID supervised and documented? Is the formal record of all the registered users maintained?

  - There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services. *(Guideline 11.2.1)*

Formal rules



Vulnerability
◊ NoOrImproperUserRegistrationAndDeRegistration

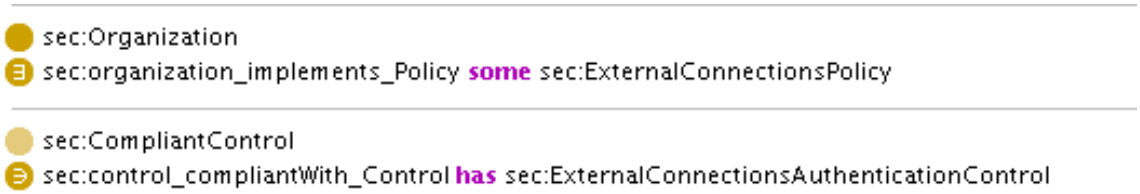
Threats
◊ UnauthorizedUseOfITSystems

- ## ExternalConnectionsAuthenticationControl

Is there a system of authentication of remote users?

  - Appropriate authentication methods should be used to control access by remote users. *(Guideline 11.4.2)*

Formal rules



New additions

SecAsset > sec:IntangibleAsset > sec:Policy > sec:ExternalConnectionsPolicy
This policy should contain information about authentication methods that should be used to control access by remote users.

Vulnerability
◊ NoExternalConnectionsAuthenticationControl

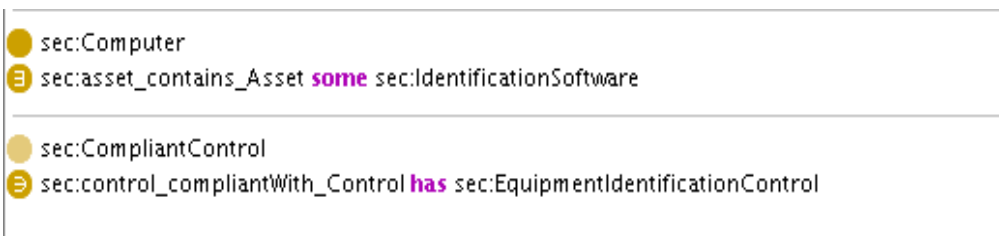
Threats
◊ BreakIn
◊ WarDriving

- ## EquipmentIdentificationControl

Is it appropriate to consider automatic equipment identification? It may be necessary to consider physical protection of the equipment to maintain the security of the equipment identifier.

  - Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment. *(Guideline 11.4.3)*

Formal Rules



New additions

sec:Asset > sec:IntangibleAsset > sec:Software > sec:IdentificationSoftware
Software that identify the equipment.This identification indicates whether this equipment is permitted to connect to the network and it should clearly indicate to which network the equipment is permitted to connect.

Vulnerability
◊ NoEquipmentIdentification

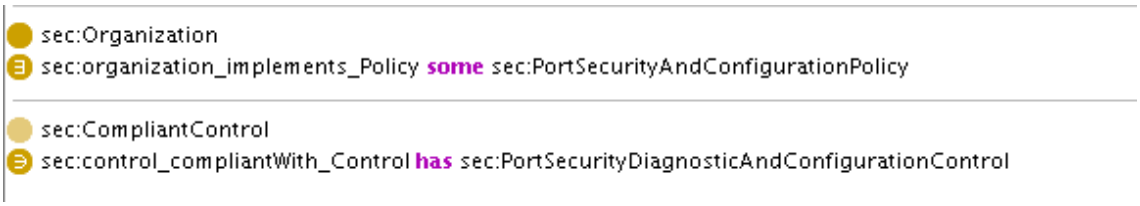
Threats
◊ UnauthorizedUseOfITSystems

- **PortSecurityDiagnosticAndConfigurationControl**

Is the physical access to diagnostic and configuration ports controlled? Is the logical access to diagnostic and configuration ports controlled?

  - Physical and logical access to diagnostic and configuration ports should be controlled. *(Guideline 11.4.4)*

Formal rules



New additions

sec:Asset > sec:IntangibleAsset > sec:Policy > sec:PortSecurityAndConfigurationPolicy
This policy should include information about physical and logical access to diagnostic and configuration ports.

Vulnerability
◊ NoPortSecurityDiagnosticAndConfiguration

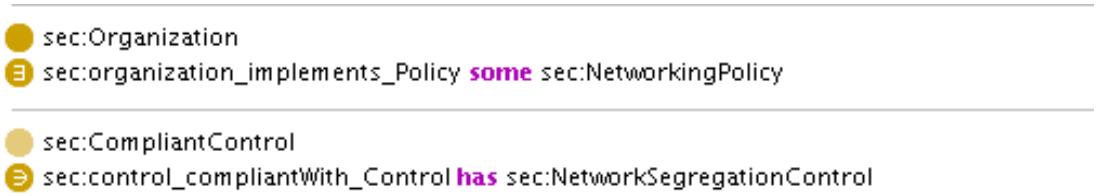
Threats
◊ UnauthorizedUseOfITSystems

- **NetworkSegregationControl**

Is the network divided into separated logical domains?

  - Groups of information services, users, and information systems should be segregated on networks. (*Guideline 11.4.5)*

Formal rules



New additions

sec:Asset > sec:IntangibleAsset > sec:Policy > sec:NetworkingPolicy
Policy should contain information about: • Design plans of the organization's network • Define routing controls. • Define security controls.

Vulnerability
◊ NoNetworkSegregation

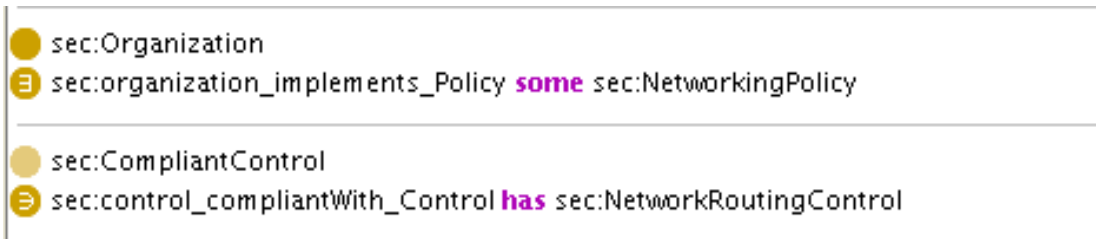
Threats
◊ UnauthorizedUseOfITSystems
◊ ProductivityDecrease

- **NetworkRoutingControl**

Are the routing controls implemented in order not to breach the access control policy?

  - Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications. (*Guideline 11.4.7)*

Formal rules



Vulnerability
◊ NoNetworkRouting

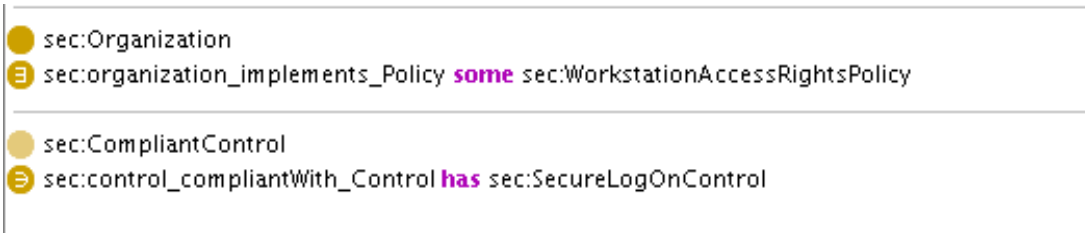
Threats
◊ UnauthorizedUseOfITSystems

- **SecureLogOnControl**

Is a procedure for logging into an operating system designed? Does it minimize the opportunity for unauthorized access? Does it disclose the minimum of information about the system?

- Access to operating systems should be controlled by a secure log-on procedure. (*Guideline 11.5.1)*

Formal rules



Vulnerability
◊ NoSecureLogOn

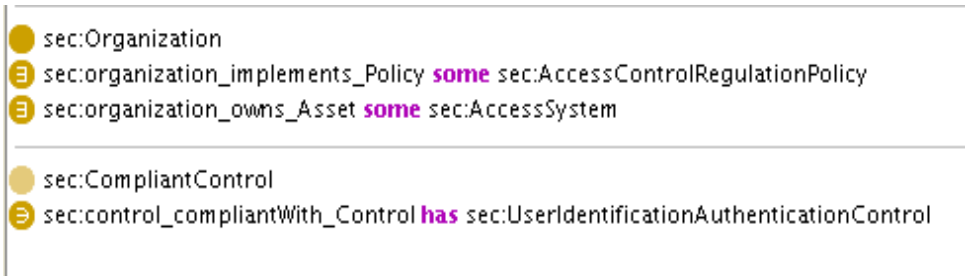
Threats
◊ UnauthorizedUseOfITSystems

- **UserIdentificationAuthenticationControl**

Are there authentication techniques to identify a user?

- All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user. (*Guideline 11.5.2)*

Formal rules



Vulnerability
◊ NoUserIdentificationAuthentication

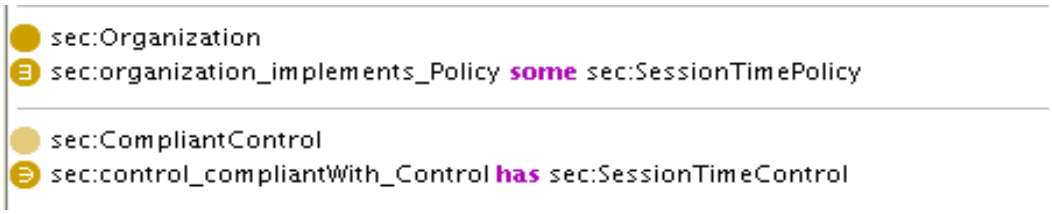
Threats
◊ UnauthorizedUseOfITSystems
◊ ElevationOfPrivileges

- **SessionTimeControl**

Are the inactive sessions shut down after a defined period of inactivity? Are there time restrictions on connection?

- Inactive sessions should shut down after a defined period of inactivity. (*Guideline 11.5.5)*
- Restrictions on connection times should be used to provide additional security for high-risk applications. (*Guideline 11.5.6)*

Formal rules



New addtions

sec:Asset > sec:IntangibleAsset > sec:Policy > sec:SessionTimePolicy
This policy should include information about: • Period of inactivity to shut down inactive sessions. • Restriccions of connections times.

Vulnerability
◊ NoSessionTime

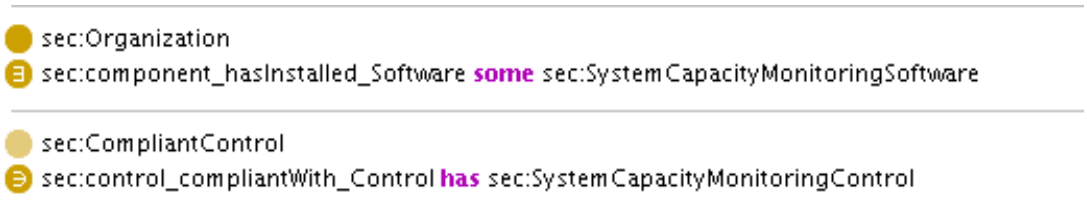
Threats
◊ UnauthorizedUseOfITSystems
◊ DataDisclosure
◊ NetworkAttack

- **SystemsTestingAndAcquisitionControl**

Is a formal testing and acquisition process followed when a new product is purchased?

  - Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls. (*Guideline 12.1.1)*

Formal procedures



New additions

sec:Asset > sec:IntangibleAsset > sec:Policy > sec:SystemsTestingAndAcquisitionPolicy
This policy should contain information about: • Requirements for new informations systems. • Requirements for enhancements to existing information systems.

Vulnerability
◊ NoSystemTesting

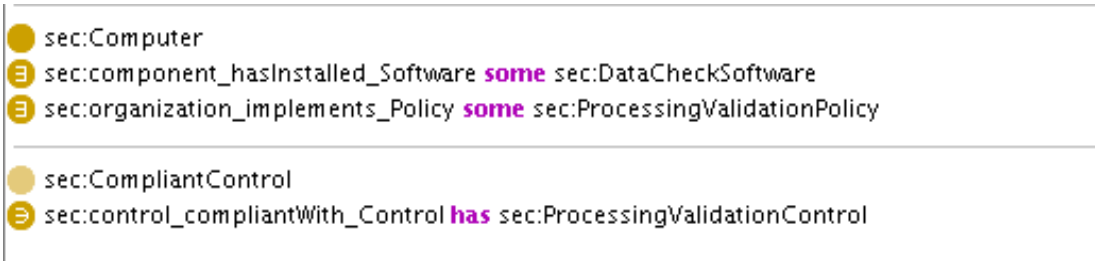
Threats
◊ HardwareFailure
◊ IncompatibleSystem
◊ ProductivityDecrease

- **ProcessingValidationControl**

Are validation checks incorporated into applications? Are validation checks applied to the input data? Are data output validated to ensure that the information storage is correct?

  - Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts. (*Guideline 12.2.3)*
  - Data input to applications should be validated to ensure that this data is correct and appropriate. (*Guideline 12.2.1)*
  - Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances. (*Guideline 12.2.4)*

Formal rules



New additions

sec:Asset > sec:IntangibleAsset > sec:Software > sec:DataCheckSoftware

sec:Asset > sec:IntangibleAsset > sec:Policy > sec:SystemsTestingAndAcquisitionPolicy
This information should include: • Internal validation controls. • Data output validation controls. • Data input validation controls.

Vulnerability
◊ NoProcessingValidation

Threats
◊ IncorrectData

- **ChangeControlProceduresControl**

Are changes controlled by formal procedures? Are these changes control procedures documented and enforced? Is a risk assessment included in this process?

  - The implementation of changes should be controlled by the use of formal change control procedures. (*Guideline 12.5.1)*

Formal rules

New additions

sec:Asset > sec:IntangibleAsset > sec:Policy > sec:ChangeControlProceduresPolicy
This policy should include information about the procedures to control and implement changes.

- **MediaAndCommunicationScanningControl**

Is the area scanned of outbound media and communications to reduce information leakage risk?

  - Scanning of outbound media and communications for hidden information to limit the risk of information leakage. *(Implementation guidance 12.5.4.a)*

Formal rules

Vulnerability
◊ NoMediaAndCommunicationScanning

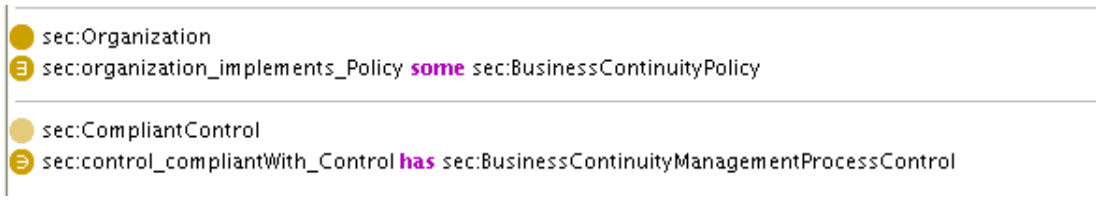
Threats
◊ DataDisclosure

- **TechnicalVulnerabilitiesControl**

Is the information about technical vulnerabilities obtained? Are the associated vulnerabilities evaluated? Are measures taken to address the associated risks?

  - Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk. *(Guideline 12.6.1)*

Formal rules



New additions

Sec:Asset > sec:IntangibleAsset > sec:Policy > sec:TechnicalVulnerabilitiesPolicy
This policy should include: a) roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking, and any coordination responsibilities required; b) information resources that will be used to identify relevant technical vulnerabilities and to maintain awareness about them should be identified for software and other technology; these information resources should be updated based on changes in the inventory, or when other new or useful resources are found; c) a timeline should be defined to react to notifications of potentially relevant technical vulnerabilities; d) once a potential technical vulnerability has been identified, the organization should identify the associated risks and the actions to be taken; such action could involve patching of vulnerable systems and/or applying other controls; e) depending on how urgently a technical vulnerability needs to be addressed, the action taken should be carried out according to the controls related to change management or by following information security incident response procedures; f) if a patch is available, the risks associated with installing the patch should be assessed (the risks posed by the vulnerability should be compared with the risk of installing the patch); g) patches should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls should be considered, such as: 1) turning off services or capabilities related to the vulnerability; 2) adapting or adding access controls, e.g. firewalls, at network borders; 3) increased monitoring to detect or prevent actual attacks; 4) raising awareness of the vulnerabilites. h) an audit log should be kept for all procedures undertaken; i) the technical vulnerability management process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency; j) systems at high risk should be addressed first.

Vulnerability
◊ NoTechnicalVulnerabilitiesControl

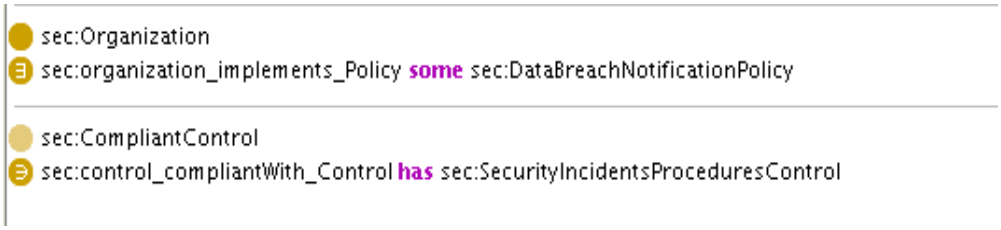
Threats
◊ HardwareFaiulure
◊ ServiceMalfunction

- ## SecurityIncidentsProceduresControl

Are the management responsibilities and procedures established to provide an effective response to information security incidents? Is there an evaluation of the incidents?

- Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents. *(Guideline 13.2.1)*
- The information gained from the evaluation of information security incidents should be used to identify recurring or high impact incidents. *(Guideline 13.2.2)*

Formal rules



Vulnerability
◊ NoSecurityIncidentsProcedures

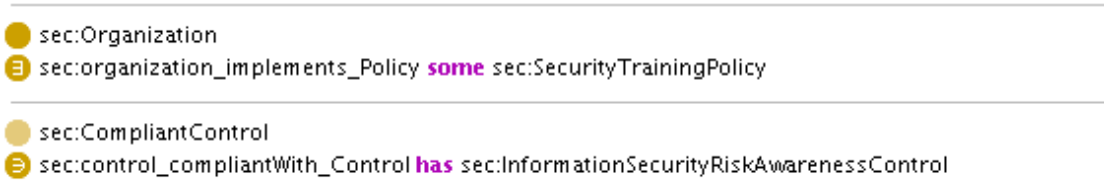
Threats
◊ UnawaredStaffMember

- ## InformationSecurityRiskAwarenessControl

Is the awareness about information security risks and their influence in the business transmitted throughout of the organization?

- Understanding the risks the organization is facing in terms of likelihood and impact in time, including an identification and prioritization of critical business processes. *(Implementation guidance 14.1.1.a)*
- Understanding the impact which interruptions caused by information security incidents are likely to have on the business (it is important that solutions are found that will handle incidents causing smaller impact, as well as serious incidents that could threaten the viability of the organization), and establishing the business objectives of information processing facilities, *(Implementation guidance 14.1.1.c)*

Formal rules



Vulnerability
◊ NoInformationSecurityRiskAwareness

Threats
◊ UnawaredStaffMember

- ## BusinessContinuityManagementProcessControl

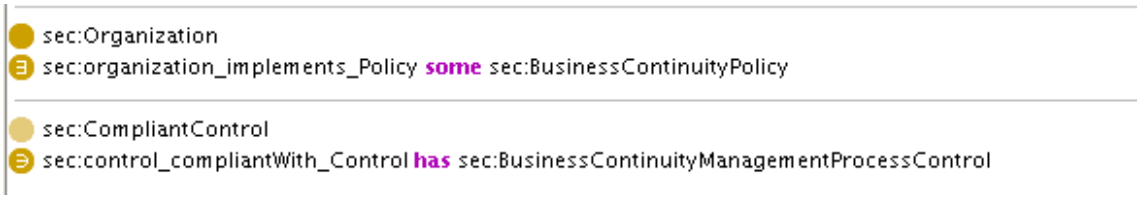
Are the information security requirements needed for the business continuity addressed by an organization managed process? Are the business continuity plans tested and updated regularly? Is there a single framework plan to ensure the consistency of all plans?

- A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity. *(Guideline 14.1.1)*
- Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes. *(Guideline 14.1.3)*
- A single framework of business continuity plans should be maintained to ensure all plans

are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance. *(Guideline 14.1.4)*

- Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective. *(Guideline 14.1.5)*

Formal rules



New additions

sec:Asset > sec:TangibleAsset > sec:Document > sec:BusinessContinuityPlans (Individual)
A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity. Plans to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.
sec:Asset > sec:IntangibleAsset > sec:Policy > sec:BusinessContinuityPolicy
Policy should contain information about: • To counteract interruptions to business activities and to protect critical business proceses from the effects of major failures of information systems or disasters and to ensure their timly resumption. • Implementation of business continuity management process to minimize the impact on theorganization and recover from loss of information assets (which may be the result of, for example natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery control. • Business impact analisys of the consequences of disasters, security failures, loss of service, and service availabilities. • Controls to identify and reduce risks, in addition to the general risks assessment process, limit the consequences of damaging incidents, and ensure that information required for business processes is readily available.

Vulnerability
◊ NoBusinessContinuityManagementProcess

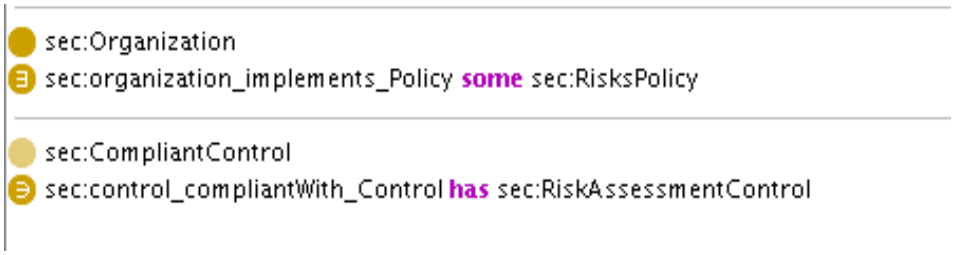
Threats
◊ FinancialLoss
◊ ReputationLoss

- ## RiskAssessmentControl

Are the risks identified? Are their probability, impact and consequences identified?

- Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security. *(Guideline 14.1.2)*

Formal rules



New additions

sec:Asset > sec:IntangibleAsset > sec:Policy > sec:RisksPolicy
Policy should include: • Risks identification. • Risks probability. • Risks probability. • Risks impact. • Risk awareness.

Vulnerability
◊ NoRiskAssessment

Threats
◊ AssetDamage
◊ AssetLoss
◊ FinalcialLoss
◊ ReputationLoss

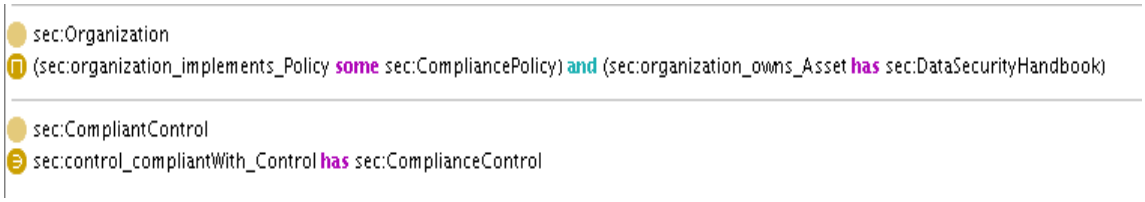
- ## ComplianceControl

Is the Information Security Policy being complied? Are all the legal, regulatory and contractual requirements and the organization's approach defined, documented and updated? Are there appropriate procedures implemented to ensure compliance with IPR on the use of property software? Is data protection and privacy in compliance with legal and contractual clauses? Are cryptographic controls in compliance with laws, agreements and regulations?

- Ensure that security activities are executed in compliance with the information security policy. *(Guideline 6.1.2)*

- All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization. *(Guideline 15.1.1)*
- Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products. *(Guideline 15.1.2)*
- Cryptographic controls should be used in compliance with all relevant agreements, laws, and regulations. *(Guideline 15.1.6)*
- Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards. *(Guideline 15.2.1)*
- Information systems should be regularly checked for compliance with security implementation standards. *(Guideline 15.2.2)*

Formal rules



New additions

sec:Asset > sec:IntangibleAsset > sec:Policy > sec:CompliancePolicy
Policy should contain information about: • Procedures to ensure the compliance of the organization's information security policy. • Define organization's approach to compliance relevant statutory, regulatory, and contractual requirements. • Procedures to define, keep up to date and ensure the compliance of relevant statutory, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

Vulnerability
◊ NoComplianceControl

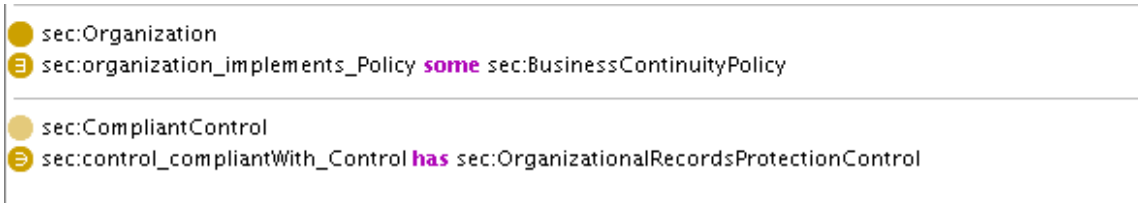
Threats
◊ HardwareFailure
◊ LegalAction

- ## OrganizationalRecordsProtectionControl

Are the organizational records protected from loss, destruction and falsification? Are they in accordance with statutory, regulatory, and business requirements?

  - Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements. *(Guideline 15.1.3)*

Formal rules



Vulnerability
◊ NoOrganizationalRecordsProtection

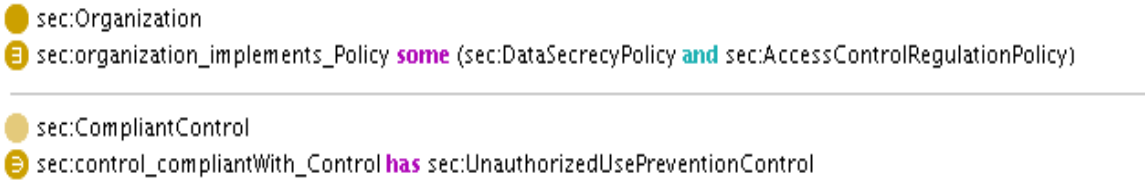
Threats
◊ AssetLoss
◊ AssetDamage
◊ FinalcialLoss
◊ ReputationLoss
◊ LegalAction

- **UnauthorizedUsePreventionControl**

  Are the users aware of the scope of their permitted access? Are there warning messages to indicate that it is not permitted the unauthorized access to the information processing facility?

  - Users should be deterred from using information processing facilities for unauthorized purposes. *(Guideline 15.1.5)*

Formal rules



Vulnerability
◊ NoUnauthorizedUsePrevention

Threats
◊ UnauthorizedPhysicalAccess
◊ UnauthorizedUseOfITSystems

CONTROL MAPPING TABLE

ISO/IEC 27002 CONTROLS	SECURITY ONTOLOGY CONTROLS New controls | Existing controls
5 SECURITY POLICY	
5.1 INFORMATION SECURITY POLICY	
5.1.1 Information security policy document	- InformationSecurityPolicyControl
5.1.2 Review of the information security policy	- InformationSecurityPolicyControl
6 ORGANIZING INFORMATION SECURITY	
6.1 INTERNAL ORGANIZATION	
6.1.1 Management commitment to information security	- SecurityManagementFrameworkControl
6.1.2 Information security co-ordination	- SecurityManagementFrameworkControl - ComplianceControl
6.1.3 Allocation of information security responsibilities	- PositionResponsabilityControl
6.1.4 Authorization process for information processing facilities	- PrivateSoftwareAndHardwareControl - NewFacilitiesAuthorizationControl
6.1.5 Confidentiality agreements	- DataSecrecyControl - InformationPassingControl
6.1.6 Contact with authorities	- AppropriateContactsControl
6.1.7 Contact with special interest groups	- AppropriateContactsControl
6.1.8 Independent review of information security	- InformationSecurityIndependentReviewControl
6.2 EXTERNAL PARTIES	
6.2.1 Identification of risks related to external parties	- ExternalStaffControl - OutsourcingControl
6.2.2 Addressing security when dealing with customers	- AccessControlRegulationControl - InternetRegulationControl
6.2.3 Addressing security in third party agreements	- ExternalStaffControl - OutsourcingControl - AccessRegulationControl - InternetRegulationControl
7 ASSET MANAGEMENT	
7.1 RESPONSIBILITY FOR ASSETS	
7.1.1 Inventory of assets	- AssetsControl - DataArchivingControl - DataDisposalControl
7.1.2 Ownership of assets	- AssetsControl - PositionResponsabilityControl
7.1.3 Acceptable use of assets	- AssetsControl - SecurityTrainingControl - InternetRegulationControl - SocialNetworkControl - MobileDeviceControl
7.2 INFORMATION CLASSIFICATION	
7.2.1 Classification guidelines	- DataArchivingControl - SensitiveInformationControl
7.2.2 Information labeling and handling	- DataArchivingControl - SensitiveInformationControl
8 HUMAN RESOURCES SECURITY	
8.1 PRIOR TO EMPLOYMENT	
8.1.1 Roles and responsibilities	- PositionResponsibilityControl
8.1.2 Screening	- StaffEmploymentControl
8.1.3 Terms and conditions of employment	- StaffEmploymentControl
8.2 DURING EMPLOYMENT	
8.2.1 Management responsibilities	- PositionResponsibilityControl
8.2.2 Information security awareness, education, and training	- SecurityTrainingControl

8.2.3 Disciplinary process	- DisciplinaryProcessControl
8.3 TERMINATION OR CHANGE OF EMPLOYMENT	
8.3.1 Termination responsibilities	- StaffDepartureControl
8.3.2 Return of assets	- StaffDepartureControl - AssetsControl
8.3.3 Removal of access rights	- StaffDepartureControl - AccessRegulationControl - AccessControlRegulationControl
9 PHYSICAL AND ENVIRONMENTAL SECURITY	
9.1 SECURE AREAS	
9.1.1 Physical security perimeter	- AccessRegulationControl - BaredWindowControl - FireSafetyControl - IntrusionAlarmSystemControl - ReceptionRegulationControl - PhysicalPerimeterProtectionControl
9.1.2 Physical entry controls	- AccessRegulationControl - AccessLogBookControl - LockedDoorsControl - SafetyDoorControl - VisitorsControl - VisibleIdentificationControl
9.1.3 Securing offices, rooms, and facilities	- PhysicalAccessKeyManagementControl - SensitiveInformationControl
9.1.4 Protecting against external and environmental threats	- FireExtinguisherControl - FireExtinguisherCriticalAreaControl - FireSafetyControl - FireSuppressionControl - EmergencyPlanningControl - RaisedFloorControl - LightningArresterControl - SmokeDetectorControl - MaterialStoringControl - PhysicalPerimeterProtectionControl
9.1.5 Working in secure areas	- SecureAreasControl
9.1.6 Public access, delivery, and loading areas	- MaterialStoringControl - DeliveryAndLoadingAreasControl
9.2 EQUIPMENT SECURITY	
9.2.1 Equipment sitting and protection	- LightningArresterControl - FireSafetyControl - EmergencyPlanningControl - AirConditioningControl - ServerPlacementControl - KensingtonLockControl - EquipmentLocationControl - EnvironmentalConditionsMonitoringControl - HumanBehaviorGuidelinesControl
9.2.2 Supporting utilities	- ElectricInstallationControl - EmergencyRecoveryControl - UninterruptiblePowerSupplyControl - UninterruptiblePowerSupplyServerControl - AirConditioningControl - WaterAlarmSystemControl - BackupMoibleITDevicesControl

9.2.3 Cabling security	- RaisedFloorControl - ElectricInstallationControl - CablingSecurityControl
9.2.4 Equipment maintenance	- MaintenanceContractControl - EmergencyPlanningControl - EmergencyRecoveryControl
9.2.5 Security of equipment off-premises	- MobileAutomaticLockingControl - MobileDeviceControl - MobileTheftProtectionControl
9.2.6 Secure disposal or re-use of equipment	- PCAndInternetRegulationControl - AntivirusSoftwareControl - MobileAntvirusControl - VirusInfectionControl - ConfigurationDataControl
9.2.7 Removal of property	- RemovableMediaControl
10 COMMUNICATIONS AND OPERATIONS MANAGEMENT	
10.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES	
10.1.1 Documented operating procedures	- DocumentedOperationalProceduresControl
10.1.2 Change Management	- SoftwareApplicationEvaluationControl
10.1.3 Segregation of duties	- PositionResponsibilityControl
10.1.4 Separation of development, test, and operational facilities	- SoftwareApplicationEvaluationControl
10.2 THIRD PARTY SERVICE DELIVERY MANAGEMENT	
10.2.1 Service delivery	- ThirdPartyServiceManagementControl - OutsourcingControl
10.2.2 Monitoring and review of third party services	- ThirdPartyServiceManagementControl
10.2.3 Managing changes to third party services	- ThirdPartyServiceManagementControl
10.3 SYSTEM PLANNING AND ACCEPTANCE	
10.3.1 Capacity management	- SystemCapacityMonitoringControl
10.3.2 System acceptance	- NewFacilitiesAuthorizationControl
10.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE	
10.4.1 Controls against malicious code	- SecurityTrainingControl - AntivirusSoftwareControl - InternetFilterControl - PCAndInternetRegulationControl - SecurityRelevantPatchesAndUpdatesControl - DataBreachNotificationControl - EmergencyRecoveryControl - InformationSecurityPolicyControl
10.4.2 Controls against mobile code	- MobileDeviceControl - MobileCodeUseBlockingControl
10.5 BACK-UP	
10.5.1 Information back-up	- BackupMoibleITDevicesControl - BackupStorageInHouseControl - BackupStorageOutsideControl - DataBackupControl - DataBackupStorageControl
10.6 NETWORK SECURITY MANAGEMENT	
10.6.1 Network controls	- PositionResponsibilityControl - AccessLogBookControl - FirewallControl - PersonalFirewallControl - WLANControl - NetworkLoggingAndMonitoringControl
10.6.2 Security of network services	- NetworkServicesAgreementControl - CloudComputingControl

10.7 MEDIA HANDLING	
10.7.1 Management of removable media	- RemovableMediaControl
10.7.2 Disposal of media	- DataDisposalControl - MediaDisposalControl
10.7.3 Information handling procedures	- DataDisposalControl - DataArchivingControl - AccessControlRegulationControl - SensitiveInformationControl
10.7.4 Security of system documentation	- AccessControlRegulationControl - SensitiveInformationControl
10.8 EXCHANGE OF INFORMATION	
10.8.1 Information exchange policies and procedures	- InformationSecurityPolicyControl
10.8.2 Exchange agreements	- ExchangeAgreementsControl
10.8.3 Physical media in transit	- PhysicalMediaInTransitControl
10.8.4 Electronic messaging	- ElectronicMessagingProtectionControl
10.8.5 Business information Systems	- InformationSecurityPolicyControl
10.9 ELECTRONIC COMMERCE SERVICES	
10.9.1 Electronic commerce	- ElectronicCommerceServicesControl
10.9.2 On-Line Transactions	- ElectronicCommerceServicesControl
10.9.3 Publicly available information	- SensitiveInformationControl
10.10 MONITORING	
10.10.1 Audit logging	- AuditLoggingAndMonitoringControl - AccessLogBookControl
10.10.2 Monitoring system use	- AuditLoggingAndMonitoringControl - DataBreachNotificationControl
10.10.3 Protection of log information	- AccessControlRegulationControl
10.10.4 Administrator and operator logs	- AuditLoggingAndMonitoringControl
10.10.5 Fault logging	- AuditLoggingAndMonitoringControl
10.10.6 Clock synchronization	- ClockSynchronizationControl
11 ACCESS CONTROL	
11.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL	
11.1.1 Access control policy	- InformationSecurityPolicyControl
11.2 USER ACCESS MANAGEMENT	
11.2.1 User registration	- UserRegistrationAndDeRegistrationControl
11.2.2 Privilege management	- DataSecrecyControl
11.2.3 User password Management	- PasswordRegulationControl
11.2.4 Review of user access rights	- WorkstationAccessRightsControl - RestrictiveGrantingOfAccessRightsControl
11.3 USER RESPONSIBILITIES	
11.3.1 Password use	- SecurityTrainingControl
11.3.2 Unattended user equipment	- SecurityTrainingControl
11.3.3 Clear desk and clear screen policy	- SecurityTrainingControl - ClearDeskControl - AutomaticLockingControl
11.4 NETWORK ACCESS CONTROL	
11.4.1 Policy on use of network services	- InformationSecurityPolicyControl
11.4.2 User authentication for external connections	- ExternalConnectionsAuthenticationControl
11.4.3 Equipment identification in networks	- AutomaticEquipmentIdentificationControl
11.4.4 Remote diagnostic and configuration port protection	- KensingtonLockControl - PortDiagnosticAndConfigurationControl
11.4.5 Segregation in networks	- NetworkSegregationControl - WLANControl
11.4.6 Network connection control	- InternetFilterControl - SocialNetworkControl
11.4.7 Network routing control	- NetworkRoutingControl

11.5 OPERATING SYSTEM ACCESS CONTROL	
11.5.1 Secure log-on procedures	- SecureLogOnControl
11.5.2 User identification and authentication	- UserIdentificationAuthenticationControl
11.5.3 Password management system	- PasswordRegulationControl
11.5.4 Use of system utilities	- PrivateSoftwareAndHardwareControl
11.5.5 Session time-out	- SessionTimeControl
11.5.6 Limitation of connection time	- SessionTimeControl
11.6 APPLICATION AND INFORMATION ACCESS CONTROL	
11.6.1 Information access restriction	- DataEncryptionControl - AccessControlRegulationControl - InformationSecurityPolicyControl
11.6.2 Sensitive system isolation	- ServerPlacementControl
11.7 MOBILE COMPUTING AND TELEWORKING	
11.7.1 Mobile computing and communications	- MobileAntvirusControl - MobileAutomaticLockingControl - MobileDeviceControl - MobileTheftProtectionControl - WLANControl
11.7.2 Teleworking	- TeleWorkingControl
12 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE	
12.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS	
12.1.1 Security requirements analysis and specification	- SystemsTestingAndAcquisitionControl
12.2 CORRECT PROCESSING IN APPLICATIONS	
12.2.1 Input data validation	- ProcessingValidationControl
12.2.2 Control of internal processing	- ProcessingValidationControl
12.2.3 Message integrity	- DataBreachNotificationControl
12.2.4 Output data validation	- ProcessingValidationControl
12.3 CRYPTOGRAPHIC CONTROLS	
12.3.1 Policy on the use of cryptographic controls	- DataEncryptionControl - DataEncryptionSoftwareControl - InformationSecurityPolicyControl
12.3.2 Key management	- DataEncryptionControl
12.4 SECURITY OF SYSTEM FILES	
12.4.1 Control of operational software	- SoftwareApplicationEvaluationControl
12.4.2 Protection of system test data	- AccessControlRegulationControl - DataArchivingControl
12.4.3 Access control to program source code	- AccessControlRegulationControl
12.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES	
12.5.1 Change control procedures	- ChangeControlProceduresControl
12.5.2 Technical review of applications after operating system changes	- SoftwareApplicationEvaluationControl
12.5.3 Restrictions on changes to software packages	- SoftwareApplicationEvaluationControl
12.5.4 Information leakage	- DataEncryptionControl - AuditLoggingAndMonitoringControl - MediaAndCommunicationScanningControl
12.5.5 Outsourced software development	- OutsourcingControl - CloudComputingControl
12.6 TECHNICAL VULNERABILITY MANAGEMENT	
12.6.1 Control of technical vulnerabilities	- SecurityUpdatesAndPatchesControl - AssetsControl - TechnicalVulnerabilitiesControl

13 INFORMATION SECURITY INCIDENT MANAGEMENT	
13.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES	
13.1.1 Reporting information security events	- DisciplinaryProcessControl - DataBreachNotificationControl
13.1.2 Reporting security weaknesses	- DataBreachNotificationControl - SecurityTrainingControl
13.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS	
13.2.1 Responsibilities and procedures	- PositionResponsibilityControl - SecurityIncidentsProceduresControl
13.2.2 Learning from information security incidents	- SecurityIncidentsProceduresControl
13.2.3 Collection of evidence	- DisciplinaryProcessControl
14 BUSINESS CONTINUITY MANAGEMENT	
14.1 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT	
14.1.1 Including information security in the business continuity management process	- InformationSecurityRiskAwarenessControl - BusinessContinuityManagementProcessControl
14.1.2 Business continuity and risk assessment	- RiskAssessmentmentControl
14.1.3 Developing and implementing continuity plans including information security	- BusinessContinuityManagementProcessControl
14.1.4 Business continuity planning framework	- BusinessContinuityManagementProcessControl
14.1.5 Testing, maintaining and re-assessing business continuity plans	- BusinessContinuityManagementProcessControl
15 COMPLIANCE	
15.1 COMPLIANCE WITH LEGAL REQUIREMENTS	
15.1.1 Identification of applicable legislation	- ComplianceControl
15.1.2 Intellectual property rights (IPR)	- ComplianceControl
15.1.3 Protection of organizational records	- OrganizationalRecordsProtectionControl
15.1.4 Data protection and privacy of personal information	- DataSecurityHandbookControl
15.1.5 Prevention of misuse of information processing facilities	- UnauthorizedUsePreventionControl
15.1.6 Regulation of cryptographic controls	- ComplianceControl
15.2 COMPLIANCE WITH SECURITY POLICIES AND STANDARDS AND TECHNICAL COMPLIANCE	
15.2.1 Compliance with security policies and standards	- ComplianceControl
15.2.2 Technical compliance checking	- ComplianceControl
15.3 INFORMATION SYSTEMS AUDIT CONSIDERATIONS	
15.3.1 Information systems audit controls	- AuditLoggingAndMonitoringControl
15.3.2 Protection of information systems audit tools	- DataEncryptionSoftwareControl