IMT4571 IT Governace Notes

Sindre Smistad

NOT PUBLISHED

HTTPS://GITHUB.COM/DOWNGOAT/IMT4571-IT-GOVERNANCE

Not Printed

Contents

1. Information Security Policy and Scope

First step of an ISMS: Define the infosec policy (should aim for a short statement of max 2 pages)

- Take into account, the organisation location, assets, technology
- Risk assessment
- Approved by managers
- Must be reviewed and updated regularly (annually)

Must answer:

- Who(does this affect)
- Everything must be agreed upon by the board and the steering group,
- Should be broad so the management and security can act without consulting the board for changes
- Might include all employees
- Possibly customers, suppliers, shareholders and other third parties
- Where (scope of the policy)
- Must be stated clearly
- Might differ from site to statedite in multi-site operation or virtual organisations
- Clearly define what parts of operation thats not included and their security implications
- What
- Availability
- Confidentiality
- Integrity
- What's important and how it is to be prioritized
- Why
- Protection of information from and wide range of threats
- Ensure business continuity, minimize business damage
- Maximize return on investments and business opportunities to maintain the competitive edge
- Cash flow profitability legal compliance and commercial image
- Should include what nature of threats faced by the organisation
- Should look up industry standard and local specific information

In addition to the policy statement there should be a plan containing

- Benefits of an ISMS
- Cost
- Expected implementation time
- When progress reviews should be done(after risk analysis, after drafts, after base implementation, after system audits, and annually)

2. The Risk Assesment and Statement of App

perational risk management is a core function on most large organisations The risk assessment should identify the threats to assets, vulnerabilities and impacts on the organization and should determine the degree of risk Every organisation is encouraged to choose the approach that is most applicable for its industry, complexity and risk environment The risk assessment must be a formal process, planned, and all input data and their analyses should be recorded Formal does not require risk assessment tools but such tools can make it less time consuming and more meaningful The techniques employed to carry out the risk assessment should be consistent with the complexity and level of assurance required by the board It is essential that the risk assessment should be done methodically systematically and comprehensively, producing comparable and reproducible results. In cases where security is already in place these should also be controlled

A risk analysis should cover

- How to eliminate risks
- Reduce risk
- Transfer them to a different organization(Insurance)

Risks can be an assessment of the economic benefits that can derive from an investment The cost of of implementing something should be significantly outweighed by economic benefits or economic loss it prevents The organisation uses risk acceptance criteria to determine what risks it is willing to tolerate. Should be clearly decided (how much economic risk will be tolerated against how much it will cost to reduce said risk) How likely is too likely against how fatal a risk could become.

Risk assessment papers are required in some places (UK) these include:

- Health and safety display screens regulations
- Personal protective equipment work regulations
- Control of substances hazardous to health regulations
- Management of health and safety at work regulations

Who conduct the risk analysis:

- Up to each individual organisation
- Annual risk assessments should be taken into consideration(someone with an updated view of threats and vulnerabilities)
- Changes in the company will need to be assessed
- Legislation, regulation and society changes

- Trusted qualified and experienced people
- Existing security/risk management roles in the organisation
- People with existing knowledge of current risks
- Can train someone internally for risk management, internal is recommended due to annual reviews
- Or Hire an external, possibly with a multiyear contract

Quantitative Risk analysis(not recommended) consists of:

- Probability of an event
- Potential loss from the event in cash
- multiply these together to get the ALE(annual loss expectancy) or EAC(Estimated annual cost)

Qualitative Risk analysis By far more widely used Does not require numerical probability data Only estimated potential loss is use Focuses on related risks, to find where most vulnerabilities and threats are found Three damage categories:

- Damage to the organization's business(competitive position, finances, reputation)
- Contractual commitments
- Legal responsibilities

Steps

- Assets: Identify all information assets and which role or department that owns it
- Threats: What threats are there for each asset
- Vulnerabilities: What can allow or make a threat possible and dangerous
- Impacts: what impact will the a threat have, if possible give a monetary value
- Risk assessment: Look at the overview and consider the likelihood of something happening, and decide what is acceptable
- Controls: Are the countermeasure to keep all risks within an acceptable terms. These controls can be:
- Directive: administrative controlsrols such as creating policies
- Preventive: protect vulnerabilities Theseo make something less likely or reduce the impact
- Detective: discover attacks and trigger preventative or corrective controls
- Corrective: Reduce the effect of an attack
- Recovery: Business continuity and disaster recovery

The cost of implementing a control should be no greater than the cost of the impact It is not possible to remove all risks

- Scope: identify the boundaries of what is to be protected
- What'Whats within the organization and what is outside
- Boundaries are physically or logically identifiable
- Witch networks, data, and locations networksed to be protected
- Parts of the organisation within the scope must bee capable of separation from their parties and from other organisations within a larger group
- Hard to implement ISMS for organisations that are not self contained, with its own board and directors, and control over its own network
- Possible for larger organisations to pursue the certification independently
- All physical premises should be listed and their networks and information assets
- Identify the assets and all systems necessary to process them
- Information assets: Informationformation systems or a body of information, files and conversations
- conversations IT systems, software(client relationship management system, payment system, mail etc.)
- IT systems, Hardware(Servers, workstations, network)

- Telecommunication systems
- Every asset have an owner who is responsibilitiesle, find these by position rather than name
- Identify the relations between the systems, the assets and the organisational objectives and tasks
- The key objectivestives with contractual or legal aspect to them should be identified in the organization's plan.
- objectives should be SMART : specific, measurable, acceptablehievable, realistic, time bound
- Find the key objectives and focus on the most important ones
- This is best done by the whole implementation team in one session
- Find what systems that are critical for the organisation tasks and objectives
- Rank systems in order of critical priority
- Give exact measures to risk categories
- Find potential threats to critical systems
- Request input from a trained information security specialist
- Can be external to the system but not necessarily the organisation
- Both intentional attackers and careless workers
- Consider links between vulnerabilitiesties and threats
- What is a threat to one system is not necessarily and threat to another one
- Categorize likelihood of occurrence
- Find potentialotential vulnerabilities
- Security weaknesses in the system
- Vulnerabilities can be exploited by threats and can lead to

Annex A of the standards have a number of controls to be considered and is the first document an inspector will want to see

- It should be review regularly
- Also used to third parties to show what degree of security that has been implemented.

the SoA (Statement of Applicability) should form the core of an ISMS manual (Example page 94)

- Works as key evidence of steps taken between risk assessment and implementation of appropriate controls
- Should not in itself contain sensitive information
- Increasing number of software tools to help automate risk management and generate the SoA

Risk treatment plan

- Identifies the appropriate management action, responsibilities and priorities for managing information security risks
- Clearly defined risk assessment process
- Include what controls are in place
- What controls where considered necessary and the timeframe for implementation
- Should include required competence and training and awareness necessary for execution and continuous improvement
- Should link all phases together (Plan,Do,Check,Act)

Measures of effectiveness, Three questions should be answered

- What is the objective of each control
- how can you determine if the control is effective
- What are the parameters that will give a positive indication of control effectiveness

Measures of effectiveness can be time consuming and should be discussed with each implemen-

tation

- Over-reliance on negative reporting is likely to result in flawed measures
- Automated monitoring is preferable to manual arrangements
- The exact aspect being measured needs to be aligned with the main objective
- The integrity of the measures or statistics being produced is of paramount importance, as management decisions are likely to be based on this information

3. Human Resources Security

Clause 5.2.1 of the standard requires the organization to provide appro- priate and adequate resources to carry out all the Plan—Do—Check—Act (PDCA) phases of information security management. Clause 5.2.2 requires that whoever is assigned an ISMS-related task has the necessary competence. These two clauses can be satisfied at the same time as the required controls are constructed. It Will be necessary to demonstrate, in the documentation, how the competences were determined, and why.

3.0.1 Job descriptions and compentency requirements

Should contain 1) a description of the competencies need 2) a statement that ever employee is requierd to be aware of the organizations info sec policy. Attetntions should be drawn to the responsibility to protect assets from unauth acces, disclosure, modification, distruction or interference. Job description should set out The clearly that breach of information security controls may be considered a mis demeanour under the organization's disciplinary policy and that breach of them might, under specific circumstances, result in dismissal.

3.0.2 Screening

Control A.8.1.2 of the standard requires the organization to carry out verification checks on permanent staff, contractors and third parties at the time of job applications. The organization should identify who will be responsible for carrying this out, how it will be done, how the data will be managed and who will have what authority in respect of the data and the recruitment process. For some roles criminal screening must be done. There are four (actually 5?) basic checks that should be completed.

1. Character reference checks, one personal and one business. Prefrably written, but might be a signed transcript of a phone call carried out by a person experienced with phone call reference checks.
2. A completness and accuracy check of the CV, usually carried out by written references supplied by previous employers. It is critical that the employer is methodical in ensuring that all facts are true.
3. Confirmation of claimed academic and professional qualifications, either by means of obtaining from the candidate copies of the certificates or other statement of qualification or through an independent CV checking service.

4. There should be an independent identity check against a passport or similar document that shows a photograph of the employee.
5. Finally, the individual's entitlement to live and work in the country should be confirmed, by reference to appropriately endorsed travel or work documents.

A draft contract can be agreeded upon but not signed before the checks are completed. In some cases if the job only deals with low level of information people can start work before checks are completed.

Organizations should have records for existing stadd of equivalent completness to those requierd for new hiers. This process should be done open and quickly, and staff should be aware of the process. If it is found that existing staff has incorrect or false CVs the organization will have to judge the exten it threatens info sec. There needs to be a procedure in places that allows new and/or inexperienced staff to have access to sensitive systems under supervision. The performance of staff that has access to sensitive information should be reviewed at least annually.

3.0.3 Terms and conditions of employment

employees, contractors and third parties all agree and sign an employment contract that contains and conditions covering their and the orgs resposibilities for info sec. It should include a confidesiality agreement that covers information acquired prior to and during employment. tandard confidentiality agreement. If loopholes are found the documents should be ammended, and if it is significat replace and re-sign existing confidentiality agreements and NDAs. The contract should make it clear that the employee has a resposibility for info sec. This resposibility must be described.

3.0.4 During employment

A organization has to ensure that employees, contractors, and thidr-party users are aware of information security threats as well as their resposibilities and liabilities, and that it has trained personell appropriately. ISO25002's includes ensuring that staff are: properly brifed on their roles and resposibilities before they are granted access to senstive information, or information systems.(information security threats, risks, and vurneabilities) All staff must appropriate awareness training and other training, as well as regular updates and communications.

Any staff involved in handling payment card data, and working within a card— holder data environment as defined by the PCI DSS, will also need specific training on their responsibilities in regard to that data.
There are also a number of staff who will require other user—specific train— ing. These include the staff identified at the beginning of this chapter as needing specific statements in their job descriptions and contracts of employment about their information security responsibilities. These include:

- the chief information officer;
- the information security adviser;
- members of the information security management forum;
- IT managers;
- network managers;
- IT and helpdesk support staff;
- webmasters;
- premises security staff
- HR, recruitment and training staff;
- general managers;

- finance staff;
- the company secretary and legal staff;
- internal quality assurance or system auditors;
- business continuity and emergecy response teams.
- basically everyone except for the cleaning lady..

Clause 5.2.2 also requires the organization to maintain records of education, training, skills, experience and qualifications, and this requirement is satisfied by following the recommendations of this chapter and attaching these records to the individual's personnel file. More importantly, the effectiveness of the training must be evaluated, and this requires the specific objectives for each piece of training, and the criteria for measuring its effectiveness, to be identified and agreed in advance. This is in line with best practice for effective staff training.

3.0.5 Disciplinary process

Employees that violate information security policies should be lashed accordingly. We will worry about finding/creating evidence of a breach later.

3.0.6 Termination or change of employment

In many organizations employment termination is sloppy information security wise, as a result the organization creates new vurnabilities. Control A.8.3.1 deals with termination responsibilities and simply requires the organization to document clearly who is responsible for performing terminations and what these responsibilities are. These responsibilities should clearly include dealing with the ongoing clauses in the contract of employment.

All organization assets should be returned, these assets fall into four catagories: software, hardware, information and knowledge. The first two asset types are best dealt with procedurally through a centralized recording and authorization process; there should be a record for eachemployee (maintained by the HR or IT department) that lists all laptops,PDAs, mobile telephones and other hardware issued to employees. This list could be linked to the asset inventory. Information - classified documents, whether electornic or paper should be returned.

Control A.8.3.3, removal of access rights, is critical, as access rights may enable a disgruntled ex—employee to compromise a system. The organization needs a clear documented procedure to ensure that upon termination access rights are also terminated, These access rightes include passwords, tokens and other authentication rights, e-mail and internet user accounts and user names, electronic files etc.

4. Physical and Environmental Security

4.1 Secure Areas

Control A.9.1 of the standard deals with secure areas. Its objective is to prevent unauthorized physical access, damage or interference to business premises and information. It has six sub-clauses. Critical or sensitive information and information processing facilities should be housed in secure areas protected by a defined secure perimeter, with appropriate security barriers (eg walls, fixed floors and ceilings, card-controlled entry gates) and controls (eg staffed reception desks) that provide protection against unauthorized access or damage to papers, media or information processing facilities. The protection implemented should be commensurate with the assessed risks and the classification of the information, and should take into account out-of—hours working and similar issues.

4.1.1 Physical security perimeter

Organizations are requierd to use a security perimeter to protect areas that contain information processing facilities. If the risk is there, more than one physical might be used to increase total protection. A line should be drawn around thepremises on the site plan, that needs to be protected. A perimeter in this context is something that povides a physical barrier between the organization and the outside world: walls, doors, windows, gates, floors, fixed ceilings (false ceilings hide a multitude of threats), skylights, etc. Special attention should also be gi ven to lifts and lift shafts, risers, maintenance and access shafts, etc. A comprehensive risk assessment should be carried out to identify the weaknesses, vulnerabilities or gaps in this perimeter. The following controls should form part of the implemented security perimeter:

- The perimeter is defined in a document, and staff are aware of what and where it is.
- The perimeter should be physically sound. There should be no gaps. External walls should be of solid construction, and doors should be protected for unauthorized access.
- There should be a staffed reception to prevent unauthorized access.
- Physical barriers should be extended from real floor to real ceiling (ie below and above any false floor or false ceiling, particularly those installed to provide effective ducting for cabling) to prevent unauthorized entry or environmental contamination such as that caused by fire or flood.
- Fire doors should open out, should slam shut, and should be alarmed. This should be advertised to prevent false alarms, there should be CCTV to watch for this.

- Appropriate intruder detection systems should be professionally installed and maintained. All external doors and accessible windows should be covered and unoccupied areas should always be alarmed. Protocol for what to do when alarm goes of should be a part of ISMS.

4.1.2 Physical Entry Controls

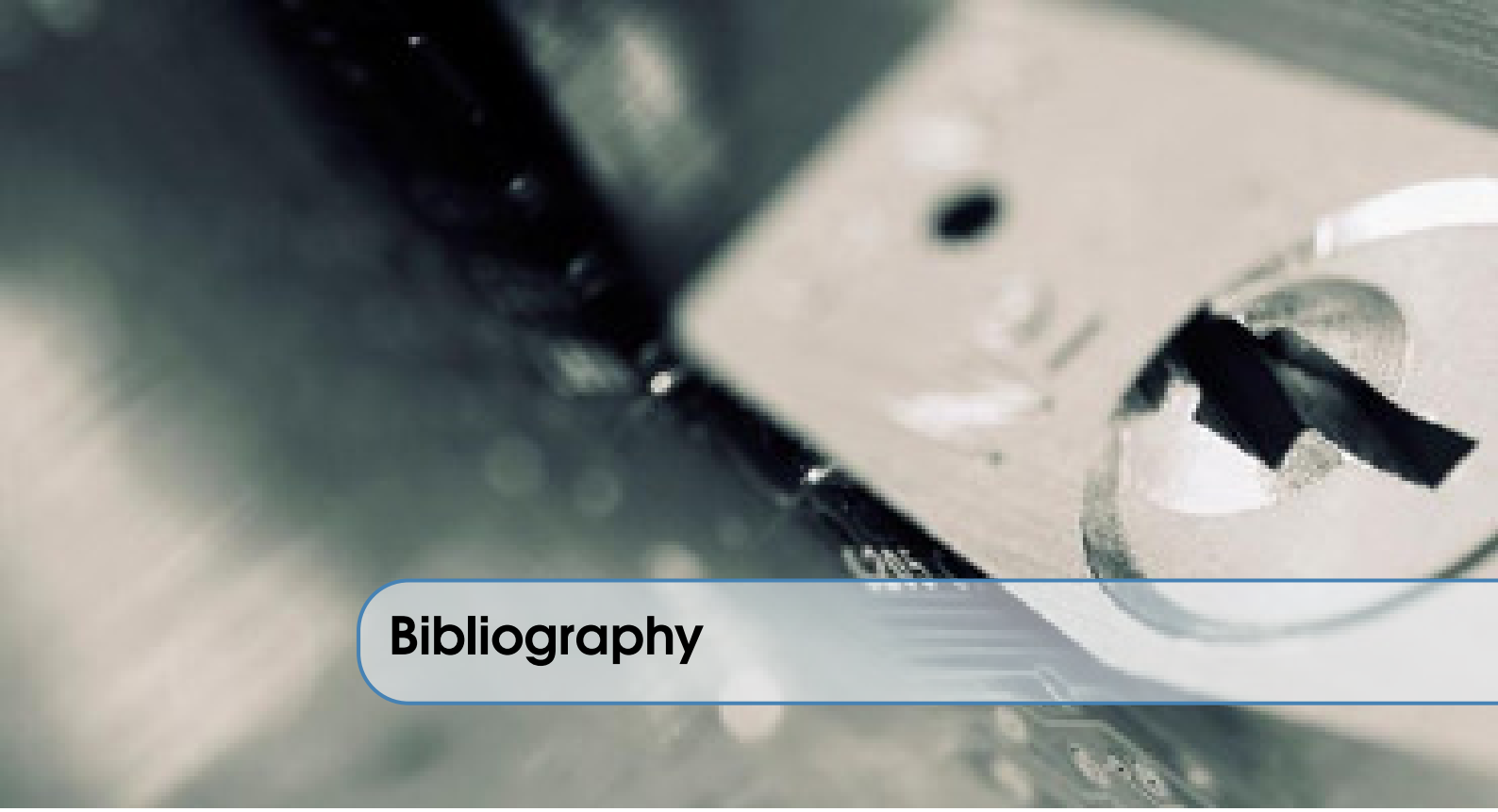
Secure areas should be protected with appropriate entry controls. ISO27002 recommends specific controls:

- Visitors should be supervised or cleared in advance. Records with time stamps of visitors should be kept.
- Outsourced security services (Securitas) should be vetted independently, and should recive trainiing on the organizations security procedures.
- If access is granted remotely there should be a communication device.
- There should be a auditable trail for usage of key cards and pins.
- Personel should be requierd to wear some visible identification.
- All staff should that might encounter Visitors should be trained so that it is difficult for a social engineer to bypass physical security controls.
- Access rights to secure areas should regularly be reviewed, updated and, where necessary, revoked, and a record of the forum's review should form part of the ISMS documentation.

4.1.3 Securing Offices, Rooms and Facilities

A secure room may cont ain lockable cabinets or safes. Secure rooms could be any rooms within the pr emises but will certainly include server rooms, telecommunications rooms and plant (power and air-conditioning) rooms. Some other (such as accounts or HR, or directors' offices) might also need to be secured. CEOs' offices should also be treated as secure rooms. Secure area design should take account of the possibility of damage from fire, flood, explosion, civil unrest and other forms of natural or humancreated disaster. The controls that ISO27002 recommends should be considered and, if appropriate, implemented include the following:

- Key storage areas and keyed entrance areas should be sited to avoid access by unauthorized persons and by the public.
- Bulding should be inobtrusive, and give little indication of their precense or purpose.
- Doors and windows should be locked when the room is unattended. Burglar bars should be considered for ground floor.
- Secure areas should be seperated from third-parties.
- Internal directories or phone books or other information about locations of secure areas should not be accessible by the public.
- Hazardous material should not be bulk stored in a secure area.
- Backup equipment should not be stored with the equipment that they will back up.



Bibliography

Books

[Smi12] John Smith. *Book title*. 1st edition. Volume 3. 2. City: Publisher, Jan. 2012, pages 123–200.

Articles

[Smi13] James Smith. “Article title”. In: 14.6 (Mar. 2013), pages 1–8.

Index