IMT4571 IT Governace Notes

Sindre Smistad

NOT PUBLISHED

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

Not Printed

Contents

1. 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.

1.0.1 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.

1.0.2 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.

1.0.3 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.

1.0.4 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.

1.0.5 Disciplinary process

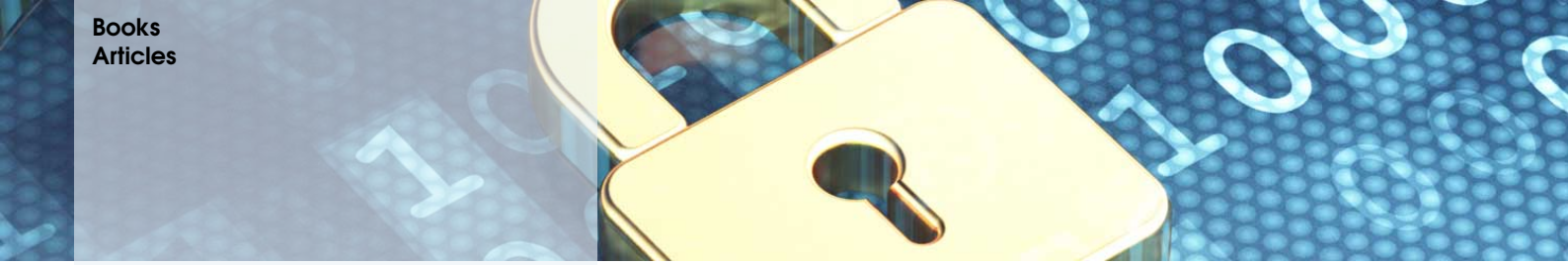
Employees that violate information security policies should be lashed accordingly. We will worry about finding/creating evidence of a breach later.

1.0.6 Termination or change of employment

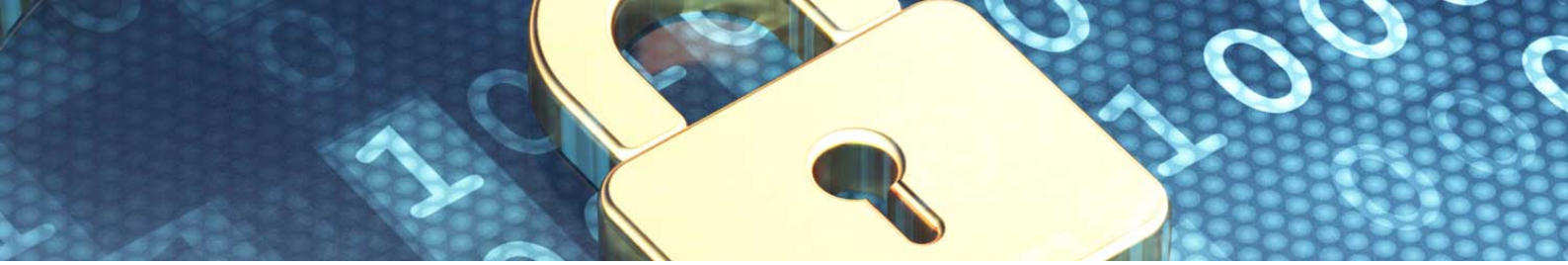
In many organizations employment termination is sloppy information security wise, as a result the organization creates new vurnabilities. Control A.8.3.1 deals with termination responsibilities and simply requires the organization to document clearly who is responsible for performing terminations and 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.



2. Physical and Environmental Security



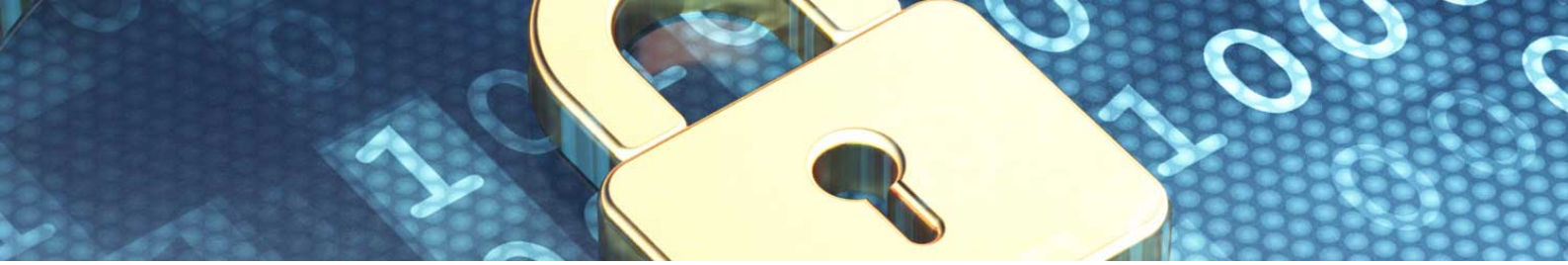
Bibliography

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