1ST EDITION

# Cybersecurity and Privacy Law Handbook

A beginner's guide to dealing with privacy and security while keeping hackers at bay

WALTER ROCCHI

# Supplementary materials

Packt audiobooks have been selected for a seamless audio experience. Some topics, however, do come with elements like images that aren't natural for this medium. We've adapted the content of the audiobooks so that you can listen to the audio without needing to refer to these visual elements unless necessary.

To give you the choice between listening to just the audio and listening to the audio while referring to the visual elements, we've created this PDF that contains all the elements that cannot translate to the audio. All references to images, tables, links, and every other visual element in the audiobook can be found within this PDF.

# To get the most out of this audiobook

I recommend obtaining a copy of the following standards/frameworks/privacy laws:

- ISO 27001 standard: https://www.iso.org/standard/54534.html
- NIST Framework: https://www.nist.gov/cyberframework
- GDPR: https://gdpr.eu/
- **Lei Geral de Proteção de Dados** (**LGPD**), Brasilian data protection law: https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd
- CCPA: https://oag.ca.gov/privacy/ccpa
- CPRA: https://thecpra.org/

# Chapter 1

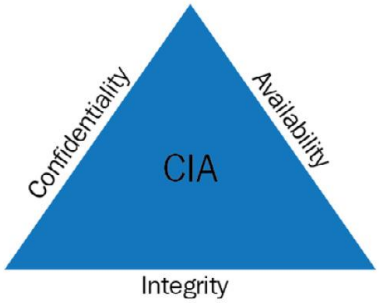


**Figure 1.1 – CIA triad**

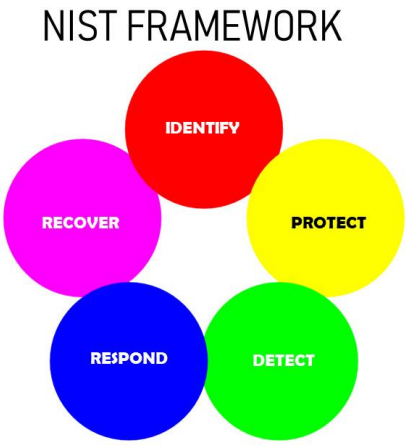


**Figure 1.2 – The five functions, Nist**

## Further Reading

- Governance: https://www.itgovernance.co.uk/

# Chapter 2

| | | | |
|---|---|---|---|
| A.15 | | | |
| Supplier relationships | | | |
| A.15.1 Information security in supplier relationships | | | |
| *Objective: To ensure the protection of the organization's assets that are accessible by suppliers* | | | |
| A.15.1.1 | Information security policy for supplier relationships<br>Information security requirements for mitigating the risks associated with the supplier's access to the organization's assets shall be agreed upon with the supplier and documented. | | *Control* |
| | Addressing security within supplier agreements<br>All relevant information security requirements shall be established and agreed upon with each supplier that may access, process, store, communicate, or provide eye-tee infrastructure components for the organization's information. | | *Control* |
| A.15.1.2 | | | |
| | | | |
| | Information and communication technology supply chain<br>Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain. | | *Control* |
| A.15.1.3 | | | |
| | | | |

**Table 2.1 – Example of control in supplier relationship (source: ISO 27001)**

| **ISO/IEC 27001 (Annex A) CONTROLS** | **Nist SP 800-53 controls** |
|---|---|
| A.5 Security policy | |
| A.5.1 Information security policy | |
| A.5.1.1 Information security policy document | XX-1 controls |
| A.5.1.2 Review of the information security policy | XX-1 controls |
| A.6 Organization of information security | |
| A.6.1 Internal | |
| A.6.1.1 Management commitment to information security | XX-1 controls, PM-2; SP 800-39, SP 800-37 |
| A.6.1.2 Information security coordination | CP-2, CP-4, IR-4, PL-1, PL-6, PM-2, SA-2; SP 800-39, SP 800-37 |
| A.6.1.3 Allocation of information security responsibilities | XX-1 controls, AC-5, AC-6, CM-9. PM-2; SP 800-39, SP 800-37 |
| A.6.1.4 Authorization process for information processing facilities | CA-1, CA-6, PM-10; SP 800-37 |
| A.6.1.5 Confidentiality agreements | PL-4, PS-6, SA-9 |
| A.6.1.6 Contact with authorities | Multiple controls with contact reference (e.g., IR-6, SI-5); SP 800-39; SP 800-37 |

| | |
|---|---|
| A.6.1.7 Contact with special interest groups | AT-5 |
| A.6.1.8 Independent review of information security | CA-2, CA-7; SP 800-39, SP 800-37 |
| A.6.2 External parties | |
| A.6.2.1 Identification of risks related to external parties | CA-3, PM-9, RA-3, SA-1, SA-9, SC-7 |
| A.6.2.2 Addressing security when dealing with customers | AC-8, AT-2, PL-4 |
| A.6.2.3 Addressing security in third-party agreements | CA-3, PS-7, SA-9 |
| A.7 Asset management | |
| A.7.1 Responsibility for assets | |
| A.7.1.1 Inventory of assets | CM-8, CM-9, PM-5 |
| A.7.1.2 Ownership of assets | CM-8, CM-9, PM-5 |
| A.7.1.3 Acceptable use of assets | AC-20, PL-4 |
| A.7.2 Information classification | |
| A.7.2.1 Classification guidelines | RA-2 |
| A.7.2.2 Information labeling and handling | AC-16, MP-2, MP-3, SC-16 |
| A.8 Human resources security | |
| A.8.1 Prior to employment | |
| A.8.1.1 Roles and responsibilities | XX-1 controls, AC-5, AC-6, AC-8, AC-20, AT-2,AT-3, CM-9, PL-4, PS-2, PS-6, PS-7, SA-9 |
| A.8.1.2 Screening | PS-3 |
| A.8.1.3 Terms and conditions of employment | AC-20, PL-4, PS-6, PS-7 |
| A.8.2 During employment | |
| A.8.2.1 Management responsibilities | PL-4, PS-6, PS-7, SA-9 |
| A.8.2.2 Awareness, education, and training | AT-2, AT-3, IR-2 |
| A.8.2.3 Disciplinary process | PS-8 |
| A.8.3 Termination or change of employment | |
| A.8.3.1 Termination responsibilities | PS-4, PS-5 |
| A.8.3.2 Return of assets | PS-4, PS-5 |
| A.8.3.3 Removal of access rights | AC-2, PS-4, PS-5 |
| A.9 Physical and environmental security | |
| A.9.1 Secure areas | |
| A.9.1.1 Physical security perimeter | PE-3 |
| A.9.1.2 Physical entry controls | PE-3, PE-5, PE-6, PE-7 |
| A.9.1.3 Securing offices, rooms, and facilities | PE-3, PE-4, PE-5 |
| A.9.1.4 Protecting against external and environmental threats | CP Family; PE-1, PE-9, PE-10, PE-11, PE-13, PE-15 |

| | |
|---|---|
| A.9.1.5 Working in secure areas | AT-2, AT-3 , PL-4, PS-6, PE-2, PE-3, PE-4, PE-6, PE-7, PE-8 |
| A.9.1.6 Public access, delivery and loading areas | PE-3 , PE-7, PE-16 |
| A.9.2 Equipment security | |
| A.9.2.1 Equipment siting and protection | PE-1, PE-18 |
| A.9.2.2 Supporting utilities | PE-1, PE-9, PE-11, PE-12, PE-14 |
| A.9.2.3 Cabling security | PE-4, PE-9 |
| A.9.2.4 Equipment maintenance | MA Family |
| ISO/IEC 27001 (Annex A) CONTROLS | Nist SP 800-53 CONTROLS |
| A.9.2.5 Security of equipment off-premises | MP-5, PE-17 |
| A.9.2.6 Secure disposal or reuse of equipment | MP-6 |
| A.9.2.7 Removal of property | MP-5, PE-16 |
| A.10 Communications and operations management | |
| A.10.1 Operational procedures and responsibilities | |
| A.10.1.1 Documented operating procedures | XX-1 controls, CM-9 |
| A.10.1.2 Change management | CM-1, CM-3, CM-4, CM-5, CM-9 |
| A.10.1.3 Segregation of duties | AC-5 |
| A.10.1.4 Separation of development, test, and operational facilities | CM-2 |
| A.10.2 Third-party service delivery management | |
| A.10.2.1 Service delivery | SA-9 |
| A.10.2.2 Monitoring and review of third-party services | SA-9 |
| A.10.2.3 Managing changes to third-party services | RA-3, SA-9 |
| A.10.3 System planning and acceptance | |
| A.10.3.1 Capacity management | AU-4, AU-5, CP-2, SA-2, SC-5 |
| A.10.3.2 System acceptance | CA-2, CA-6, CM-3, CM-4, CM-9, SA-11 |
| A.10.4 Protection against malicious and mobile code | |
| A.10.4.1 Controls against malicious code | AC-19, AT-2, SA-8, SC-2, SC-3, SC-7, SC-14, SI-3, SI-7 |
| A.10.4.2 Controls against mobile code | SA-8, SC-2, SC-3, SC-7, SC-14, SC-8, SC-18 |
| A.10.5 Backup | |
| A.10.5.1 Information backup | CP-9 |
| A.10.6 Network security management | |
| A.10.6.1 Network controls | AC-4, AC-17, AC-18, AC-20, CA-3, CP-8, PE-5,SC-7, SC-8, SC-9, SC-10, SC-19, SC-20, SC-21, SC-22, SC-23 |
| A.10.6.2 Security of network services | SA-9, SC-8, SC-9 |

| | |
|---|---|
| A.10.7 Media handling | |
| A.10.7.1 Management of removable media | MP Family, PE-16 |
| A.10.7.2 Disposal of media | MP-6 |
| A.10.7.3 Information handling procedures | MP Family, SI-12 |
| A.10.7.4 Security of system documentation | MP-4, SA-5 |
| A.10.8 Exchange of information | |
| A.10.8.1 Information exchange policies and procedures | AC-1, AC-3, AC-4, AC-17, AC-18, AC-20, CA-3, PL-4, PS-6, SC-7, SC-16, SI-9 |
| A.10.8.2 Exchange agreements | CA-3, SA-9 |
| A.10.8.3 Physical media in transit | MP-5 |
| A.10.8.4 Electronic messaging | Multiple controls; electronic messaging not addressed separately in SP 800-53 |
| A.10.8.5 Business information systems | CA-1, CA-3 |
| A.10.9 Electronic commerce services | |
| A.10.9.1 Electronic commerce | AU-10, IA-8, SC-7, SC-8, SC-9, SC-3, SC-14 |
| A.10.9.2 Online transactions | SC-3, SC-7, SC-8, SC-9, SC-14 |
| A.10.9.3 Publicly available information | SC-14 |
| A.10.10 Monitoring | |
| A.10.10.1 Audit logging | AU-1, AU-2, AU-3, AU-4, AU-5, AU-8, AU-11, AU-12 |
| A.10.10.2 Monitoring system use | AU-1, AU-6, AU-7, PE-6, PE-8, SC-7, SI-4 |
| A.10.10.3 Protection of log information | AU-9 |
| A.10.10.4 Administrator and operator logs | AU-2, AU-12 |
| A.10.10.5 Fault logging | AU-2, AU-6, AU-12, SI-2 |
| A.10.10.6 Clock synchronization | AU-8 |
| A.11 Access control | |
| A.11.1 Business requirement for access control | |
| A.11.1.1 Access control policy | AC-1, AC-5, AC-6, AC-17, AC-18, AC-19, CM-5, MP-1, SI-9 |
| A.11.2 User access management | |
| A.11.2.1 User registration | AC-1, AC-2, AC-21, IA-5, PE-1, PE-2 |
| A.11.2.2 Privilege management | AC-1, AC-2, AC-6, AC-21, PE-1, PE-2, SI-9 |
| A.11.2.3 User password management | IA-5 |

**Table 2.2**

It's important to note that, as stated on their website, this document from NIST is available for free at https://doi.org/10.6028/Nist.SP.800-53r5.

# Chapter 3

- The entire text of *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002* can be found here: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058.

# Chapter 4

- Article 29: Very useful in this regard is this guide, to which you are referred: https://www.hldataprotection.com/2013/04/articles/international-eu-privacy/article-29-working-party-gives-new-guidance-on-purpose-limitation/

# Chapter 5

## Figures

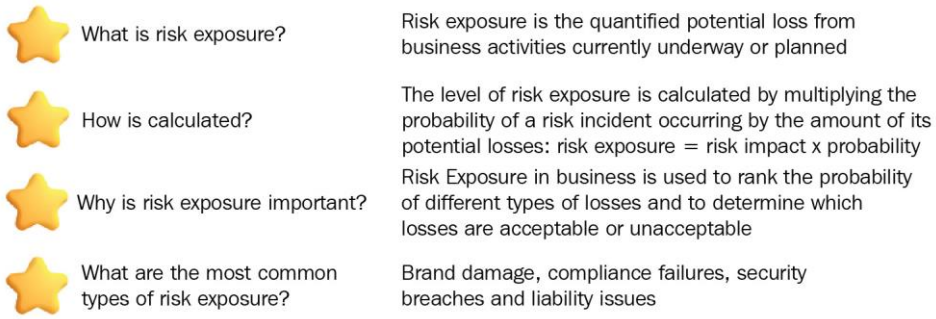


**Figure 5.1 – Factors related to risk exposure**

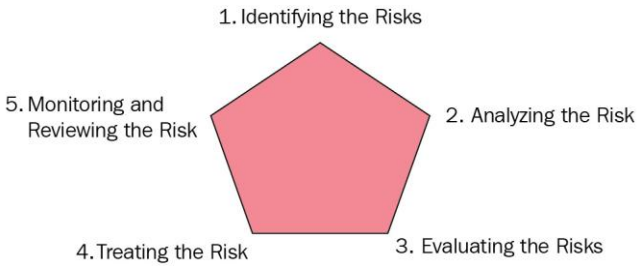


**Figure 5.2 – Risk management steps**

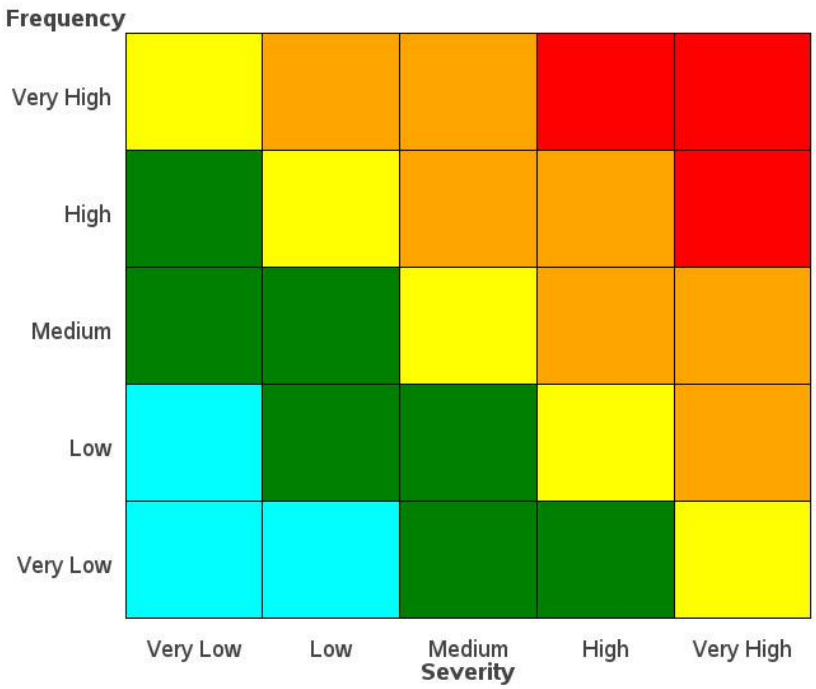


**Figure 5.3 – A risk management heatmap**

## Further Reading

- eBIOS: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_ebios.html

# Chapter 6

## Figures


Figure 6.1 – Plan-Do-Check-Act

## Tables

| Audience | Type of Training |
|---|---|
| Users | User awareness training |
| iSMS governance | Those in charge of the implementation |
| Information security manager | The individual who supervises implementation |
| Service desk | • Normal user and access management<br>• IT security employees in charge of event and incident management |
| Human resource | Responsibilities for employee recruiting, training, and termination |
| IT support personnel | • Incident response management<br>• Secure operations |
| Executives | iSMS support |

Table 6.1 – Audience and level/type of training

# Chapter 7

## Figures

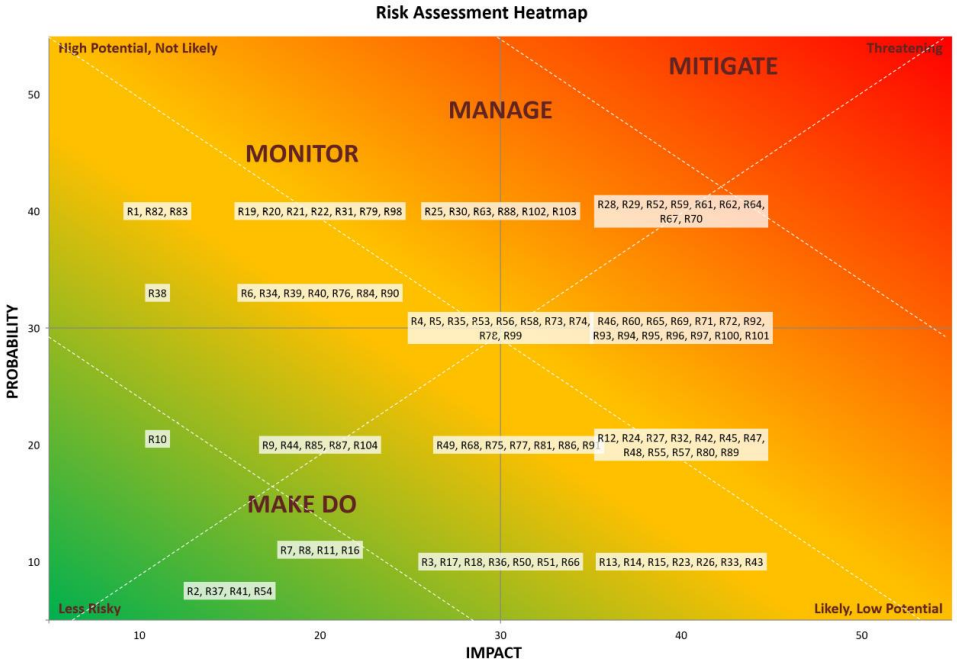


**Figure 7.1 – Risk assessment heatmap**

## Tables

| | | | LIKELIHOOD | | | |
|---|---|---|---|---|---|---|
| | | | 10 Low | 20 Medium | 30 High | 40 Very High |
| IMPACT | 10 | Low | 4 | 1 | 1 | 3 |
| | 20 | Medium | 4 | 5 | 7 | 7 |
| | 30 | High | 7 | 7 | 10 | 6 |
| | 40 | Very High | 7 | 12 | 14 | 9 |

**Table 7.1 – Heatmap in tabular format**

# Chapter 8

## Tables

| Person in charge | Action |
|---|---|
| | Gathering information |
| Writer responsibility | Writing the process |
| | Sharing the draft with stakeholders |
| | |
| | Reviewing a draft |
| Stakeholder responsibility | Submitting comments and corrections |
| | |
| Writer responsibility | Creating the final draft |
| | |
| Manager (business unit) | Approving the final version |

**Table 8.1**

## Further Reading

- Twitter's privacy policy: https://twitter.com/en/privacy

# Chapter 10

- **Cloud Security Alliance** (or **CSA**): https://cloudsecurityalliance.org/
- **European Cloud User Coalition** (**ECUC**): https://ecuc.group/
- **ECUC** related questions: https://ecuc.group/
- **BSI C5** of the German Federal Office for Information Security: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_Einfuehrung/C5_Einfuehrung_node.html
- CSA**,** a cloud computing environment: https://www.cloudsecurityalliance.org

# Chapter 11

- There is no silver bullet to create acceptable data protection, as an old FTC blog post reiterates: https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework

# Appendix

- Enforcement tracker: https://www.enforcementtracker.com/
- GDPR-CARPA: https://edpb.europa.eu/news/national-news/2022/cnpd-adopts-certification-mechanism-gdpr-carpa_en