

Theme 2 Pre-Reading Packet: Strategic Governance, Risk, and Compliance Foundations & Taxonomy



Dr Diarmuid Ó Briain
Version: 1.0

Copyright © 2026 C²S Consulting

Licensed under the EUPL, Version 1.2 or – as soon they will be approved by the European Commission - subsequent versions of the EUPL (the "Licence");

You may not use this work except in compliance with the Licence.

You may obtain a copy of the Licence at:

https://joinup.ec.europa.eu/sites/default/files/custom-page/attachment/eupl_v1.2_en.pdf

Unless required by applicable law or agreed to in writing, software distributed under the Licence is distributed on an "AS IS" basis, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the Licence for the specific language governing permissions and limitations under the Licence.

Dr Diarmuid Ó Briain



Table of Contents

1 Objectives.....	4
2 Introduction.....	4
3 Cyber Crime Classifications.....	5
3.1 Classifications of Cyber Crimes.....	5
3.2 Specific Cyber crimes.....	6
4 Intellectual Property Foundations.....	8
4.1 Patent / Trademark / Copyright / Trade Secret.....	8
5 Privacy & Workplace Law Taxonomy.....	11
5.1 Data Privacy.....	11
5.2 Examples of Privacy Laws.....	11
5.3 Privacy at Work.....	14
6 High-Level Regulatory Standards.....	15
6.1 Regulatory Compliance.....	15
6.2 Financial Industry Compliance (Basel II and III).....	16
6.3 Business Ethics.....	17
7 Basic Risk Taxonomy.....	18
7.1 What is Risk?.....	18
7.2 Risk Assessment Process.....	18
7.3 Risk Terminology (Asset, Exposure, Likelihood).....	19
8 Bibliography.....	21

Table of Figures

Figure 1: Linking Risk Terminology.....	19
Figure 2: Risk Management Process.....	20

Index of Tables

Table 1: Privacy Summary.....	13
Table 2: Regulatory Compliance.....	17

1 Objectives

By the end of this Pre-Reading Packet (PRP), you will be able to:

- Deconstruct the phases of a cyber attack from initial reconnaissance and credential exploitation through lateral movement, obfuscation, and data exfiltration.
- Differentiate between automated authentication exploits, specifically brute force and dictionary attacks, while identifying the predictable patterns that weaken user passwords.
- Explain the network mechanics of Denial of Service (DoS) and masquerading vectors, contrastingly evaluating SYNchronise (SYN) floods, Smurf amplification, and Man-in-the-Middle (MitM) traffic interception.
- Deploy, baseline, and validate a secure Kali Linux virtual infrastructure, establishing safe hypervisor network translation modes and verifying upstream connectivity via the command line.

 **Important Notice for Students:** This document contains the foundational definitions, legal frameworks, and risk taxonomies required for Theme 2 (Governance, Risk, and Compliance). You are expected to master this material independently; it will be directly tested in the Theme 2 Individual Readiness Assurance Test (iRAT).

2 Introduction

In the previous topics under Theme 1, the technical core of Operational Technology (OT) and logical security architectures were deconstructed. However, building technically secure environments is useless if they exist in a vacuum. To protect critical infrastructure, an organisation must possess a unified strategy to direct its actions, evaluate its threats, and abide by the law.

This is the role of **Governance, Risk, and Compliance (GRC)**. The GRC represents the structural boundaries of security programmes.

This PRP establishes the foundational elements required for the interactive topics. By mastering these key definitions, from cybercrime categories and intellectual property boundaries to the basic taxonomy of risk equations, are necessary prepare for real-world GRC scenarios, including risk registers and the construction of an ISO 27001 compliance framework.

3 Cyber Crime Classifications

Computer crime encompasses a broad range of potentially illegal activities. It is generally divided into one of two types of categories:

- Crimes that target computer networks or devices directly
 - Malware (malicious code)
 - Denial Of Service (DoS) attacks
 - Computer viruses
- Crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device:
 - Cyber stalking
 - Fraud and identity theft
 - Phishing scams
 - Information warfare

A computer can be a source of evidence. Even though the computer is not directly used for criminal purposes, it is an excellent device for record keeping, particularly given the power to encrypt the data. If this evidence can be obtained and decrypted, it can be of great value to criminal investigators.

3.1 Classifications of Cyber Crimes

Cybercrimes in general can be classified into four categories:

- **Individual Cyber Crimes**
 - This type of cybercrime targets individuals. It includes phishing, spoofing, spam, cyberstalking, and more.
- **Organisation Cyber Crimes**
 - The main target here are organisations. Usually, this type of crime is carried out by teams of criminals including malware attacks and DoS attacks.
- **Property Cybercrimes**
 - Such cybercrimes target property such as credit cards or even intellectual property rights.
- **Society Cybercrimes**
 - This is the most dangerous form of cybercrime as it includes cyber-terrorism.

3.2 Specific Cyber crimes

The following cyber crimes are most prevalent in OT environments:

- **Phishing and Scam**
 - OT environments are often targeted by phishing attacks, as employees in these environments may have access to sensitive data and systems. Phishing emails can be used to trick employees into revealing confidential information or clicking on malicious links that can infect their computers with malware.
- **Ransomware Attacks**
 - Ransomware attacks are also a major threat to OT environments. Ransomware can encrypt critical data and systems, making them unavailable to operators. This can disrupt operations and lead to significant financial losses.
- **Hacking/Misusing Computer Networks**
 - Hackers may target OT environments to gain unauthorised access to systems and data, or to disrupt operations. This can be done for a variety of reasons, including financial gain, espionage, or sabotage.
- **OT-Specific Attacks**
 - There are also a number of OT-specific cyber attacks that can target OT environments. These attacks may exploit vulnerabilities in OT devices or protocols to gain access to systems, disrupt operations, or cause physical damage.

In addition to the above, other cyber crimes that can be prevalent in OT environments include:

- **Social Engineering Attacks**
 - Social engineering attacks are attempts to trick employees into revealing confidential information or performing actions that compromise security. These attacks can be very effective, as they exploit human psychology.
- **Malware Attacks**
 - Malware is malicious software that can be used to infect computers and systems. Malware can be used to steal data, disrupt operations, or cause physical damage.
- **DOS Attacks**
 - DoS attacks are attempts to make computer systems or networks unavailable to their intended users. DoS attacks can be used to disrupt operations or extort money from victims.
- **Cyber terrorism**
 - There is a growing concern among law enforcement that Internet problems and server scans are part of an organised effort by cyber terrorists, foreign intelligence services, or other groups to map potential security holes in critical systems.

It is important to note that the cyber threat landscape is constantly evolving, and new threats are emerging all the time. Organisations with OT environments need to be aware of the latest threats and take steps to mitigate them. This includes implementing security measures such as firewalls, intrusion detection systems, and access control lists. Organisations should also train their employees on cyber security best practices.

4 Intellectual Property Foundations

Is a term referring to a number of distinct types of legal monopolies over creations of the mind, both artistic and commercial, and the corresponding fields of law. Under intellectual property law, owners are granted certain exclusive rights to a variety of intangible assets, such as musical, literary, and artistic works; discoveries and inventions; and words, phrases, symbols, and designs. Common types of intellectual property include copyrights, trademarks, patents, industrial design rights and trade secrets in some jurisdictions.

4.1 Patent / Trademark / Copyright / Trade Secret

4.1.1 Patent



This term refers to a right granted to anyone by the state (Government patent office) who invents or discovers any new and useful process, machine, article of manufacture, or composition of matter, or any new and useful improvement thereof.

A patent provides the right to exclude others from making, using, selling, offering for sale, or importing the patented invention for the term of the patent, which is usually 20 years from the filing date subject to the payment of maintenance fees.

Patents are the strongest form of IP and is a legally enforceable right to prevent others from using the invention for the period of the patent.

4.1.2 Trademark



A trademark is a distinctive sign or indicator used by an individual, business organisation, or other legal entity to identify that the products or services to consumers with which the trademark appears originate from a unique source, and to distinguish its products or services from those of other entities.

A trademark is designated by the following symbols:

- TM Unregistered trade mark
- SM Unregistered service mark
- ® Registered trademark

The owner of a registered trademark may commence legal proceedings for trademark infringement to prevent unauthorised use of that trademark. However, registration is not required. The owner of a common law trademark may also file suit, but an unregistered mark may be protectable only within the geographical area within which it has been used or in geographical areas into which it may be reasonably expected to expand.

A service mark differs from a trademark in that the mark is used on the advertising of the service rather than on the packaging or delivery of the service, since there is generally no "package" to place the mark on, which is the practice for trademarks.



4.1.3 Copyright

Copyright is a form of intellectual property that gives the author of an original work exclusive right for a certain time period in relation to that work, including its publication, distribution and adaptation, after which time the work is said to enter the public domain. Copyright applies to any expressible form of an idea or information that is substantive and discrete and fixed in a medium.

Copyright protection extends to the following works:

- original literary, dramatic, musical or artistic works
- sound recordings and films
- broadcasts and TV programmes
- the typographical arrangement of published editions
- computer programmes
- original databases.

Copyright takes effect as soon as the work is put on paper, film, or other fixed medium such as CD-ROM, DVD, Internet, etc. No protection is provided for ideas while the ideas are in a person's mind. Copyright law protects the form of expression of ideas, not the ideas themselves.

Copyright is a weaker IP right than a patent but its duration is much longer. It typically applies for 50 – 70 years depending on the form of work.



4.1.3.1 Copyleft

Copyleft is a play on the word copyright to describe the practice of using copyright law to remove restrictions on distributing copies and modified versions of a work for others and requiring that the same freedoms be preserved in modified versions.

Copyleft is a form of licensing and can be used to modify copyrights for works such as computer software, documents, music and art. In general, copyleft licensing scheme, give every person who receives a copy of a work permission to reproduce, adapt or distribute the work as long as any resulting copies or adaptations are also bound by the same copyleft licensing scheme.

Common practice for using copyleft is to codify the copying terms for a work with a licence. Any such licence typically gives each person possessing a copy of the work the same freedoms as the author, including (from the Free Software Definition):

- the freedom to use the work
- the freedom to study the work
- the freedom to copy and share the work with others
- the freedom to modify the work, and the freedom to distribute modified and therefore derivative works

The GNU General Public Licence, originally written by Richard Stallman, was the first copyleft licence to see extensive use, and continues to dominate the licensing of copylefted software.

4.1.4 Trade Secret

A trade secret is information that:

- Is not generally known to the public
- Confers some sort of economic benefit on its holder
- Is the subject of reasonable efforts to maintain its secret?

A company can protect its confidential information through non-competitive and Non-Disclosure Agreements (NDA) with its employees. The law of protection of confidential information effectively allows a perpetual monopoly in secret information. It does not expire as would a patent. The lack of formal protection, however, means that a third party is not prevented from independently duplicating and using the secret information once it is discovered.

5 Privacy & Workplace Law Taxonomy

Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively.

5.1 Data Privacy

This refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data about one's self. Privacy concerns exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. In some cases these concerns refer to how data is collected, stored, and associated. In other cases the issue is who is given access to information. Other issues include whether an individual has any ownership rights to data about them, and/or the right to view, verify, and challenge that information. Various types of personal information often come under privacy concerns:

- Financial privacy
- Internet privacy
- Medical privacy
- Sexual privacy
- Political privacy

5.2 Examples of Privacy Laws

5.2.1 The EU

The ***EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*** [1] was the initial EU directive which regulated the processing of personal data within member states. It was replaced by ***Regulation (EU) 2016/679 General Data Protection Regulation (GDPR)*** [2] as a new EU law on data protection and privacy in the Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. The regulation came into effect in May 25, 2018.

GDPR regulates the processing of personal data by both public and private organisations, including the transfer of personal data outside the EU. It gives individuals more control over their personal data and requires organisations to be more transparent about how they collect and use personal data.

5.2.2 The UK

The UK equivalent of the GDPR is the **UK Data Protection Act 2018 (UK GDPR)** [3]. It is the UK's implementation of the EU GDPR, which is a regulation in EU law on data protection and privacy. The UK GDPR came into force on 28 June 2018, the same day that the UK left the EU.

The UK GDPR is almost identical to the EU GDPR, but it makes some minor changes to reflect UK law. For example, the UK GDPR includes a definition of "special category data" that is slightly broader than the definition in the EU GDPR.

Like the EU GDPR, the UK GDPR applies to all organisations that process personal data of individuals in the UK, regardless of whether the organisation is based in the UK or not. It also applies to organisations that offer goods or services to individuals in the UK, or that monitor the behaviour of individuals in the UK.

5.2.3 The US

Due to the different legal tradition in the US, compared to the EU, which places a greater emphasis on individual liberty and less emphasis on government regulation means that the US is less inclined to adopt comprehensive data protection laws. There is no single federal data protection law similar to GDPR; however, there are a number of federal and state laws that regulate the collection, use, and disclosure of personal data. Examples include the **California Consumer Privacy Act (CCPA), 2018** [4] and the **Virginia Consumer Data Protection Act (VCDPA), 2023** [5]. These laws give consumers the right to know what personal data is collected about them, to request access to that data, to have it deleted, and to opt out of the sale of their personal data. Similar laws exist in other US states such as Colorado, Connecticut and Utah; however, each of these laws vary in scope and complexity, but they all give consumers some rights over their personal data.

Apart from the state laws there are a number of federal laws that protect specific types of personal data, such as the **Health Insurance Portability and Accountability Act (HIPAA), 1996** [6] protects health data, the **Gramm-Leach-Bliley Act (GLBA), 1999** [7] protects financial data, the **Fair Credit Reporting Act (FCRA) 1970** [8] protects credit data, while the **Children's Online Privacy Protection Act (COPPA), 1998** [9] protects the personal data of children under the age of 13.

Since GDPR came into force, in Europe, there is growing support for a federal data protection law in the US. In 2022, the American Data Privacy and Protection Act (ADPPA), 2022 [10] passed through a committee of the US Congress with bipartisan support; however, it was never brought to a vote in the House of Representatives. The aim of ADPPA is to create a single federal data protection law for the US.

5.2.4 India

The **Indian Digital Personal Data Protection Act (DPDP), 2023** [11] is a comprehensive data protection law that was passed by the Indian Parliament in August 2023. It is similar to the EU GDPR in many ways. It gives individuals rights over their personal data and also requires organisations that process personal data to take steps to protect it and to ensure that it is processed in a fair and lawful way.

There are also some key differences between the DPDP Act and the GDPR. For example, the DPDP Act does not have a requirement for organisations to obtain explicit consent from individuals before processing their personal data. Additionally, the DPDP Act exempts certain types of organisations from its provisions, such as government agencies and small businesses.

The DPDP Act is enforced by the Data Protection Authority (DPA), which is a new independent body that has been set up under the Act. The DPA has the power to investigate complaints about breaches of the DPDP Act and to take action against organisations that are found to be in breach.

5.2.5 Privacy Summary

Table 1 provides a comparison of various data protection regulations and acts from different countries and regions.

Table 1: Privacy Summary

Document	Year	Body	Specific Purpose
Regulation (EU) 2016/679 General Data Protection Regulation (GDPR)	2016	EU	Addresses the transfer of personal data outside the EU and EEA areas.
UK Data Protection Act 2018 (UK GDPR)	2018	UK	Implements EU GDPR regulations in the UK.
Health Insurance Portability and Accountability Act (HIPAA)	1996	US	Protects health data.
Gramm-Leach-Bliley Act (GLBA)	1999	US	Protects financial data.
Fair Credit Reporting Act (FCRA)	1970	US	Protects credit data.
Children's Online Privacy Protection Act (COPPA)	1998	US	Protects the personal data of children under the age of 13.
Digital Personal Data Protection Act (DPDP), 2023	2023	India	Comprehensive data protection law that is similar to the EU GDPR.

5.3 Privacy at Work

Today companies are under increasing pressure to monitor employees electronically, and workers should assume they are being watched. A large percentage of companies are now conducting some form of *active monitoring* of their employees, particularly E-mail monitoring.

Employees generally have a right to privacy based on a '*reasonable expectation of privacy*' but a written policy notifying employees of monitoring lifts somewhat the expectation of privacy.

This means that if an employee is led to expect something is private, such as e-mail communications, then that privacy cannot be violated. But, if the company informs its employees that, for example, e-mail sent over the company's network is monitored, then the employee can no longer claim an expectation of privacy.

The key for successfully managing the balancing act between privacy and security is for firms to make clear to their employees that their privacy at work is limited.

It's not really about Big Brother watching either, e-mail is quite often used as a tool of harassment and employers have a duty to be sure harassment isn't being propagated. For the company to exercise its responsibility it needs to monitor or at least record the e-mail traffic.

6 High-Level Regulatory Standards

6.1 Regulatory Compliance

Historically in all countries there have been periods of business and government excesses and subsequent legal, public and political reaction. All countries have imposed regulation of compliance to prevent and punish companies who participate in corporate malpractice.

6.1.1 The EU

Directive (EU) 2006/43/EC, the Audit Directive [12]. The Audit Directive sets out minimum standards for the statutory audit of Public-Interest Entities (PIE) in the EU. The directive requires PIEs to have their annual financial statements audited by an independent auditor and to publish a corporate governance statement.

In addition to the EU Audit Directive, there are a number of other EU laws and regulations that are relevant to corporate governance and anti-corruption. For example, the **Regulation (EU) 596/2014, the Market Abuse Regulation** [13] prohibits insider trading and market manipulation and the **Regulation (EU) 2016/679 General Data Protection Regulation (GDPR)** [2] sets out rules for the processing of personal data.

Companies operating in the EU should be aware of all of the relevant EU laws and regulations, and should take steps to ensure that they are in compliance.

6.1.2 The UK

The **UK Bribery Act 2010** [14], is a law that makes it illegal to bribe anyone, anywhere in the world. It is one of the toughest anti-bribery laws in the world and applies to all UK companies and individuals, regardless of where they are located or operating. The Bribery Act creates four offences:

- Bribery of another person
- Bribery of a foreign public official
- Failure of a commercial organisation to prevent bribery
- Bribery of a foreign public official to obtain or retain business or an advantage in the conduct of business.

The Act also introduces strict liability for commercial organisations whose employees or other associated persons engage in bribery, even if the organisation itself did not know about or benefit from the bribery. This means that commercial organisations must have adequate procedures in place to prevent bribery.

The Bribery Act has been successful in reducing bribery in the UK. Since it came into force, the Serious Fraud Office (SFO) has prosecuted over 200 individuals and companies for bribery offences.

6.1.3 The US

The **US Foreign Corrupt Practices Act (FCPA)** [15] is an anti-bribery provision makes it unlawful for a US citizen, and certain foreign issuers of securities, to make a corrupt payment to a foreign official for the purpose of obtaining or retaining business for or with, or directing business to, any person. The law also requires publicly traded companies to maintain records that accurately and fairly represent the company's transactions. It also requires these companies to have an adequate systems of internal accounting controls.

The **US Sarbanes–Oxley Act (SOX)** [16] is the US Public Company Accounting Reform and Investor Protection Act. It was enacted as a reaction to a number of major corporate and accounting scandals such as at Enron and a number of other US companies which cost investors billions of dollars when the share prices of affected companies collapsed, shook public confidence in the nation's securities markets.

The legislation sets standards for all US public company boards, management and public accounting firms. It does not apply to privately held companies. The act contains 11 titles, or sections, ranging from additional corporate board responsibilities to criminal penalties, and requires the Securities and Exchange Commission (SEC) to implement rulings on requirements to comply with the new law.

Additionally, the **US Gramm-Leach-Bliley Act (GLBA)** [7] is the US Financial Services Modernisation Act to allow commercial banks, investment banks, securities firms and insurance companies to consolidate. One area of the act is the protection of the privacy of consumer information held by these organisations.

6.1.4 India

There are a number of Indian laws and regulations that are relevant to corporate governance and anti-corruption. The **Prevention of Corruption Act, 1988 (POCA)** [17] criminalises bribery and other forms of corruption while the **Companies Act, 2013 (CA)** [18] sets out standards for corporate governance and financial reporting.

6.2 Financial Industry Compliance (Basel II and III)

Basel II [19] is a series of recommendations on banking laws and regulations are issued by the Basel Committee on Banking Supervision. This international committee encourages contacts and cooperation among its members and other banking supervisory authorities. Basel II creates an international standard that banking regulators can use when creating regulations about how much capital banks need to put aside to guard against the types of financial and operational risks banks face. Generally speaking, these rules mean that the greater risk to which the bank is exposed, the greater the amount of capital the bank needs to hold to safeguard its solvency and overall economic stability.

Basel III [20] augmenting and superseding parts of the Basel II standards, it was developed in response to the deficiencies in financial regulation revealed by the financial crisis of 2007–08. It is intended to strengthen bank capital requirements by increasing minimum capital requirements, holdings of high quality liquid assets, and decreasing bank leverage.

6.2.1 Regulatory Compliance Summary

Table 2 provides an overview of various regulations and acts related to corporate governance, financial crime, and data protection from different jurisdictions.

Table 2: Regulatory Compliance

Document	Year	Body	Specific Purpose
Directive (EU) 2006/43/EC, the Audit Directive	2006	EU	Sets out minimum standards for the statutory audit of Public-Interest Entities (PIE) in the EU.
Regulation (EU) 596/2014, the Market Abuse Regulation	2014	EU	Prohibits insider trading and market manipulation.
Regulation (EU) 2016/679 General Data Protection Regulation (GDPR)	2016	EU	Sets out rules for the processing of personal data.
Bribery Act 2010	2010	UK	Makes it illegal to bribe anyone, anywhere in the world.
Foreign Corrupt Practices Act (FCPA)	1977	US	Anti-bribery provision makes it unlawful for a US citizen, and certain foreign issuers of securities, to make a corrupt payment to a foreign official.
Sarbanes–Oxley Act (SOX)	2002	US	US Public Company Accounting Reform and Investor Protection Act.
Gramm-Leach-Bliley Act (GLBA)		US	Protects financial data.
Prevention of Corruption Act, 1988 (POCA)	1988	India	Criminalises bribery and other forms of corruption.
Companies Act, 2013 (CA)	2013	India	Sets out standards for corporate governance and financial reporting.

6.3 Business Ethics

Business or corporate ethics is a form of applied ethics examining moral principles and problems within a business environment. It applies to all aspects of business conduct, influencing both individuals and organizations as a whole. The volume of ethical issues reflects how much business practices are perceived to conflict with non-economic social values.

To address this, many companies establish internal policies regarding employee conduct. Whether phrased in broad terms or detailed as specific behavioural codes, these guidelines clarify organizational expectations and guide workers through common ethical dilemmas. Fostering these policies promotes greater ethical awareness, ensures consistent behaviour, and helps avoid major corporate crises.

Additionally, an increasing number of companies require employees to attend business conduct seminars covering policies, case studies, and legal mandates. Some even require workers to sign formal agreements committing to abide by these codes of conduct.

7 Basic Risk Taxonomy

7.1 What is Risk?

Risk is a function of the **likelihood** of a given **threat-source's** exercising a particular potential **vulnerability**, and the resulting **impact** of that adverse event on the organisation [21].

7.2 Risk Assessment Process

It is important to emphasise that risk assessment is a process as opposed to a once off event. Because technology and processes change, risk assessments need to be conducted periodically.

- **Phase 1: Preliminary Risk Assessment**
 - In the first phase, it is necessary to perform a preliminary risk assessment and educate upper management about the risks so that they can make informed decisions about where to allocate the necessary resources.
- **Phase 2: Risk Analysis of Critical Areas and Processes**
 - In the second phase a more in-depth set of risk assessments are performed on critical areas and processes identified in the preliminary risk assessment.
- **Phase 3: Organisation-Wide Risk Assessment**
 - The goal of the third phase is to perform a thorough, wide risk assessment.
 - This phase focuses on IT issues relating to risk assessment with the understanding that this is only part of the process. Ultimately, risk assessment must take into account natural disasters, fire, and other events that can make a system unavailable.

7.3 Risk Terminology (Asset, Exposure, Likelihood)



Figure 1: Linking Risk Terminology

- **Asset:** Anything within the environment that should be protected.
- **Asset Valuation:** Monetary value of an asset. This value should include not just the physical value of the item but costs associated with development, maintenance, repair and replacement for example.
- **Threats:** Anything that may cause an undesirable outcome for the organisation of a specific asset. This includes any action or in-action that could cause damage, loss, disclosure of assets.
- **Vulnerability:** Absence or weakness of safeguards that protect an organisation or asset.
- **Exposure:** Being susceptible to an asset loss because of a threat. Exposure is not a realised threat but the fact that a vulnerability exists and it could be exposed.
- **Risk:** Possibility that a threat will exploit a vulnerability to cause harm to an asset.
- **Safeguards:** A safeguard is a countermeasure that removes a vulnerability or protects an asset from all or specific threats.
- **Attack:** The actual exploitation of a vulnerability that may cause damage, loss or disclosure of assets.
- **Breach:** A breach is the occurrence of a security mechanism being bypassed or thwarted.

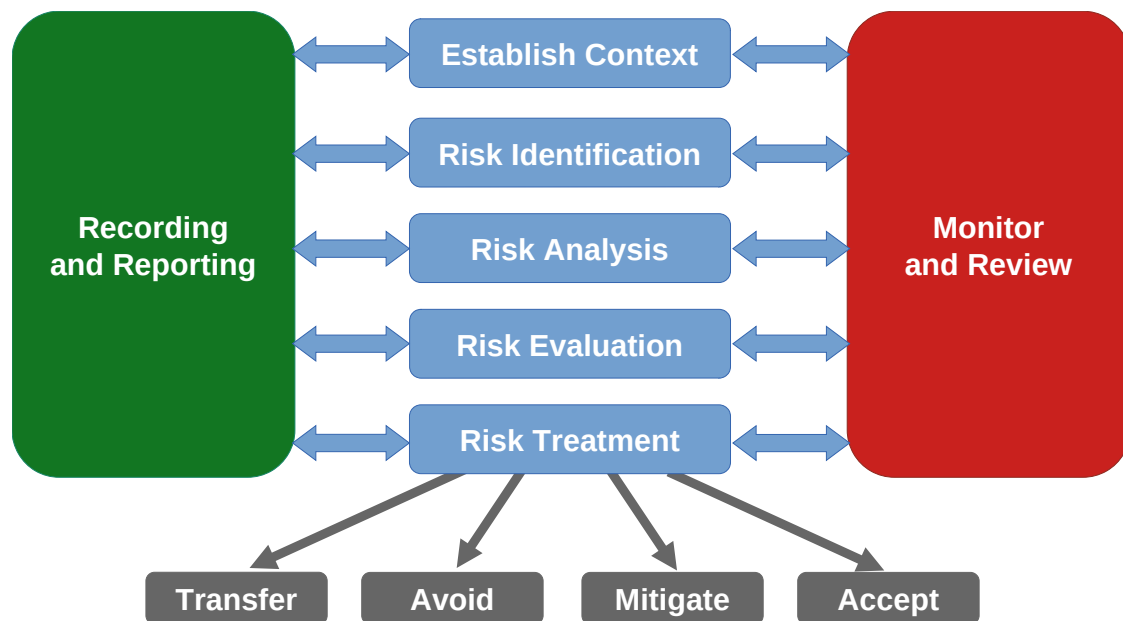


Figure 2: Risk Management Process

Risk Management plays an important role in maintaining the cybersecurity posture of an organisation. It involves identifying, analysing, evaluating, and mitigating potential risks that could impact the objectives or the successful execution of business operations [22].

Risk management is a fundamental practice across various industries, including finance, healthcare, engineering, project management, and more. It is an ongoing process, and as circumstances change, new risks are identified and mitigated. As a result, a proactive and adaptable approach to risk management plays a crucial role in long-term success.

Figure 2 summarises *International Organisation for Standardisation (ISO) 31000:2018 – Risk Management Guidelines* which provides a good reference for understanding the Risk Management Process. It involves:

- Establishing the Scope, context and criteria
- Risk Identification
- Risk Analysis
- Risk Evaluation
- Risk Treatment
- Monitoring and review
- Recording and Reporting

8 Bibliography

- [1] EU Directive 95/46/EC, *EU protection of individuals with regard to the processing of personal data and on the free movement of such data*. 1995. Accessed: Mar. 10, 2003. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046>
- [2] Regulation (EU) 2016/679, *EU General Data Protection Regulation (GDPR)*. 2016. Accessed: Mar. 10, 2020. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [3] UK, *UK Data Protection Act 2018*. 2018. Accessed: Sep. 30, 2023. [Online]. Available: <https://www.legislation.gov.uk/ukpga/1990/18/contents>
- [4] USA, *US California Consumer Privacy Act (CCPA) 2018*. 2018. Accessed: Sep. 30, 2023. [Online]. Available: https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
- [5] USA, *US Virginia Consumer Data Protection Act (VCDPA) 2023*. 2023. Accessed: Sep. 30, 2023. [Online]. Available: <https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/>
- [6] USA, *US Health Insurance Portability and Accountability Act (HIPAA) 1996*. 1996. Accessed: Sep. 30, 2023. [Online]. Available: <https://www.cdc.gov/phlp/publications/topic/hipaa.html>
- [7] USA, *US Gramm-Leach-Bliley Act (GLBA) (Financial Services Modernization Act) 1999*. 1999. Accessed: Sep. 30, 2023. [Online]. Available: <https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act>
- [8] USA, *US Fair Credit Reporting Act (FCRA) 1970*. 1970. Accessed: Sep. 30, 2023. [Online]. Available: <https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act>
- [9] USA, *US Children's Online Privacy Protection Act (COPPA) 1998*. 1998. Accessed: Sep. 30, 2023. [Online]. Available: <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>
- [10] USA, *US American Data Privacy and Protection Act (ADPPA), 2022 (Not passed into law)*. 2022. Accessed: Sep. 30, 2023. [Online]. Available: <https://www.congress.gov/bill/117th-congress/house-bill/8152>
- [11] India, *Indian Digital Personal Data Protection Bill, 2023*. 2023. Accessed: Sep. 30, 2023. [Online]. Available: <https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023>
- [12] Directive (EU) 2006/43/EC, *EU Audit Directive*. 2006. Accessed: Oct. 09, 2023. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0043>
- [13] Regulation (EU) No 596/2014, *EU Market Abuse (market abuse regulation)*. 2014. Accessed: Oct. 09, 2023. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0596&qid=1696372229904>
- [14] UK, *UK Bribery Act 2010*. 2010. Accessed: Sep. 30, 2023. [Online]. Available: <https://www.legislation.gov.uk/ukpga/2010/23/introduction>
- [15] USA, *US Foreign Corrupt Practices Act (FCPA) 1977*. 1977. Accessed: Sep. 30, 2023. [Online]. Available: <https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act>
- [16] USA, *US Sarbanes–Oxley Act (SOX) 2002*. 2002. Accessed: Sep. 30, 2023. [Online]. Available: <https://www.govinfo.gov/content/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf>
- [17] India, *Indian Prevention of Corruption Act (POCA) 1988*. 1988. Accessed: Sep. 30, 2023. [Online]. Available: <https://www.indiacode.nic.in/bitstream/123456789/1558/1/A1988-49.pdf>
- [18] India, *Indian Companies Act (CA) 2013*. 2013. Accessed: Sep. 30, 2023. [Online]. Available: https://www.indiacode.nic.in/handle/123456789/2114?sam_handle=123456789/1362
- [19] 'Basel II Accord'. Jun. 2004.
- [20] *Basel III*, Jun. 01, 2011. Accessed: Oct. 03, 2023. [Online]. Available: <https://www.bis.org/publ/bcbs189.htm>
- [21] NIST SP 800-30, 'Guide for Conducting Risk Assessments', National Institute of Standards and Technology, Oct. 2012. Accessed: Aug. 22, 2023. [Online]. Available: <https://www.nist.gov/privacy-framework/nist-sp-800-30>
- [22] ISO 31000:2018, *ISO 31000:2018: Risk management — Guidelines*, Feb. 2018. Accessed: Oct. 10, 2023. [Online]. Available: <https://www.iso.org/standard/65694.html>

This page is intentionally blank