

# **L7: Data Security, Governance and Compliance (ACCA7028)**

Apply the principles and practices of Data security, Governance and Compliance based on a given scenario.

Student: Austin Hooper (1700481)  
MSc Software Engineering and Artificial Intelligence

**Wales Institute for Science and Art (WISA)**  
**University of Wales Trinity Saint David**

Lecturer: Dr Carlene Campbell  
January 12<sup>th</sup> 2021

## Table of Contents

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| 1. Introduction .....                                                   | 1  |
| 2. Security Frameworks Literature Review (Task 1) .....                 | 2  |
| 2.1. Updating Standards and Regulations for Good Practice .....         | 2  |
| 2.2. NIST Cybersecurity Framework.....                                  | 3  |
| 2.3. ISO/IEC 27000 Series .....                                         | 6  |
| 2.4. IASME Governance Standard for Information and Cyber Security ..... | 8  |
| 2.5. CIS Controls Framework .....                                       | 11 |
| 3. Security Framework Design (Task 2).....                              | 14 |
| 3.1. Framework Design Influences .....                                  | 14 |
| 3.2. Case Scenario Relevance .....                                      | 15 |
| 3.3. Framework Resources for CaribbeanCoffee .....                      | 16 |
| 4. Conclusion and Future Work .....                                     | 19 |
| References .....                                                        | 20 |
| Background Reading .....                                                | 25 |

## Table of Figures

|                                                                   |    |
|-------------------------------------------------------------------|----|
| Figure 1: 27001 brief control measure example [26].....           | 6  |
| Figure 2: 27002 detailed control measure example [27, p. 5] ..... | 7  |
| Figure 3: Proposed framework specificity and scope .....          | 16 |
| Figure 4: Proposed framework hierarchy .....                      | 16 |
| Figure 5: The developed framework order of implementation.....    | 18 |

## Table of Tables

|                                                                                |    |
|--------------------------------------------------------------------------------|----|
| Table 1: NIST CSF categories [17, p. 23] .....                                 | 4  |
| Table 2: NIST CSF example criteria for the identity category [17, p. 24] ..... | 5  |
| Table 3: 27001/27002 clauses.....                                              | 7  |
| Table 4: IASME Governance Standard categories .....                            | 9  |
| Table 5: IASME and NIST framework mappings .....                               | 9  |
| Table 6: IASME Governance Framework risk profiles [33, p. 16] .....            | 10 |
| Table 7: CIS Framework control example [44, p. 22].....                        | 11 |
| Table 8: CIS Framework implementation groups [44, p. 5].....                   | 12 |
| Table 9: CIS controls by category .....                                        | 12 |
| Table 10: Framework Core .....                                                 | 17 |

## **Abstract**

Information security is an increasingly complex field which must be addressed at both organisational and technical levels. This research set out to develop a custom information security framework for the CaribbeanCoffee case scenario. To inform framework design, four frameworks were critiqued, analysed, and compared. The benefits and drawbacks of these frameworks, along with other academics' approaches, were considered when designing the framework. The framework resources developed consist of the framework core, an order of implementation flow diagram, hierarchy and scope diagram. The framework core consists of six categories: Identify, Educate, Implement, Review, Preserve, and Recover, each with three sub-categories. The framework targets the key issues in the case scenario, while remaining open to adaptation. Future work could involve reviewing a wider range of frameworks and literature and developing more detailed technical guidance for each sub-category of the framework.

# 1. Introduction

Information security (InfoSec) frameworks are becoming increasingly essential as cyber threats increase in frequency and severity. An information security framework is defined as a specification of a model to follow during the design and implementation of security controls, InfoSec policies, education, and training [1, p. 412]. An Information Security Management System (ISMS) is part of an organisation's overall management system, providing a systematic approach for managing an organisation's security [2], [3], often developed using or alongside an InfoSec framework.

This research investigates a variety of security frameworks to inform the design of a custom security approach for the CaribbeanCoffee case scenario. Section 2 investigates the structure and content of four security frameworks, analysing, comparing, and critiquing them, along with discussing the need to constantly update security standards. Section 3 discusses the design of a security approach based on the research conducted in Section 2. Section 4 concludes the report.

## **2. Security Frameworks Literature Review (Task 1)**

This section discusses the importance of updating security standards, along with reviewing four security frameworks, critiquing, analysing, and comparing them, to make informed decisions when designing a security framework in Section 3.

### **2.1. Updating Standards and Regulations for Good Practice**

It is essential for organisations to continuously update their regulations, standards, and frameworks. By doing so, organisations ensure they remain compliant with current legislation to reduce the organisation's liability. This, in turn, reduces the potential risk to the organisation's reputation with its customers and stakeholders [4]. This can also provide a competitive advantage over organisations without proven consideration of InfoSec issues. An example of this is the recent plethora of websites updating their privacy policies to comply with the General Data Protection Regulation (GDPR), or in some cases, the UK Data Protection Act 2018 [5, p. 53] - the UK's implementation of the GDPR [6]. Specifically, this was to comply with GDPR Article 12's requirement for organisations to be transparent about their use of subjects' data [7, pp. 39–40], as discussed by the Information Commissioner's Office [8, p. 19].

Another reason for the need to keep standards up to date is to protect against new and emerging cybersecurity threats and attack vectors in a dynamic and evolving industry [9]–[11]. As a result of this, organisations reduce the risk of their information's integrity [9] and comply better with the concepts of the Confidentiality, Integrity, and Availability (CIA) triad.

Continuous updating of standards also allows organisations to revise their procedures as the use of technology changes, creating new challenges [12]. One example is the increasing popularity of Bring Your Own Device (BYOD) schemes – the technology has not changed, but the culture and way in which staff use it has evolved [13], [14]. As a result, new measures must be put into place, requiring updates to regulations. Another example is the emergence of new security concerns due to the rise in working from home due to the Coronavirus pandemic [15].

## 2.2. NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework, (“NIST CSF”), is a voluntary framework which provides general guidance for implementing cybersecurity controls, with more specific guidance provided by other sources and frameworks [16], [17]. The NIST CSF has a significant element of self-assessment [17, pp. 20–21], [18], [19], and takes a risk-based approach to managing cybersecurity. It aids organisations in describing their current cybersecurity state, their target state, and to identify opportunities for improvement [17, pp. 2–4].

The NIST CSF consists of [18], [19]:

- Framework Core - a set of cybersecurity activities, outcomes, and references. The Framework Core’s categories are shown in Table 1, along with an example of its criteria in Table 2. The five activities, named as “functions” in the framework document, are listed below:
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover
- Framework Implementation Tiers – provide context on how an organisation views cybersecurity risks, along with the measures in place to prevent them. These tiers are effectively rankings for the level of sophistication employed by the organisation depending on their needs. The four tiers are as follows:
  - Tier 1: Partial
  - Tier 2: Risk Informed
  - Tier 3: Repeatable
  - Tier 4: Adaptive
- Framework Profiles – represent the outcomes based on the organisation’s business needs. Profiles can be used to identify opportunities for improving cybersecurity, by comparing the “Current” profile with a “Target” profile, as discussed in the framework [17, p. 4].

Table 1: NIST CSF categories [17, p. 23]

| Function Unique Identifier | Function | Category Unique Identifier | Category                                        |
|----------------------------|----------|----------------------------|-------------------------------------------------|
| ID                         | Identify | ID.AM                      | Asset Management                                |
|                            |          | ID.BE                      | Business Environment                            |
|                            |          | ID.GV                      | Governance                                      |
|                            |          | ID.RA                      | Risk Assessment                                 |
|                            |          | ID.RM                      | Risk Management Strategy                        |
|                            |          | ID.SC                      | Supply Chain Risk Management                    |
| PR                         | Protect  | PR.AC                      | Identity Management and Access Control          |
|                            |          | PR.AT                      | Awareness and Training                          |
|                            |          | PR.DS                      | Data Security                                   |
|                            |          | PR.IP                      | Information Protection Processes and Procedures |
|                            |          | PR.MA                      | Maintenance                                     |
|                            |          | PR.PT                      | Protective Technology                           |
| DE                         | Detect   | DE.AE                      | Anomalies and Events                            |
|                            |          | DE.CM                      | Security Continuous Monitoring                  |
|                            |          | DE.DP                      | Detection Processes                             |
| RS                         | Respond  | RS.RP                      | Response Planning                               |
|                            |          | RS.CO                      | Communications                                  |
|                            |          | RS.AN                      | Analysis                                        |
|                            |          | RS.MI                      | Mitigation                                      |
|                            |          | RS.IM                      | Improvements                                    |
| RC                         | Recover  | RC.RP                      | Recovery Planning                               |
|                            |          | RC.IM                      | Improvements                                    |
|                            |          | RC.CO                      | Communications                                  |

Table 2: NIST CSF example criteria for the identity category [17, p. 24]

| Function                | Category                                                                                                                                                                                                                                                                                    | Subcategory                                                                                                                                                             | Informative References                                                                                                                                                                            |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IDENTIFY</b><br>(ID) | <b>Asset Management (ID.AM):</b><br>The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. | <b>ID.AM-1:</b> Physical devices and systems within the organization are inventoried                                                                                    | CIS CSC 1<br>COBIT 5 BAI09.01, BAI09.02<br>ISA 62443-2-1:2009 4.2.3.4<br>ISA 62443-3-3:2013 SR 7.8<br>ISO/IEC 27001:2013 A.8.1.1, A.8.1.2<br>NIST SP 800-53 Rev. 4 CM-8, PM-5                     |
|                         |                                                                                                                                                                                                                                                                                             | <b>ID.AM-2:</b> Software platforms and applications within the organization are inventoried                                                                             | CIS CSC 2<br>COBIT 5 BAI09.01, BAI09.02, BAI09.05<br>ISA 62443-2-1:2009 4.2.3.4<br>ISA 62443-3-3:2013 SR 7.8<br>ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1<br>NIST SP 800-53 Rev. 4 CM-8, PM-5 |
|                         |                                                                                                                                                                                                                                                                                             | <b>ID.AM-3:</b> Organizational communication and data flows are mapped                                                                                                  | CIS CSC 12<br>COBIT 5 DSS05.02<br>ISA 62443-2-1:2009 4.2.3.4<br>ISO/IEC 27001:2013 A.13.2.1, A.13.2.2<br>NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8                                             |
|                         |                                                                                                                                                                                                                                                                                             | <b>ID.AM-4:</b> External information systems are catalogued                                                                                                             | CIS CSC 12<br>COBIT 5 APO02.02, APO10.04, DSS01.02<br>ISO/IEC 27001:2013 A.11.2.6<br>NIST SP 800-53 Rev. 4 AC-20, SA-9                                                                            |
|                         |                                                                                                                                                                                                                                                                                             | <b>ID.AM-5:</b> Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value | CIS CSC 13, 14<br>COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02<br>ISA 62443-2-1:2009 4.2.3.6<br>ISO/IEC 27001:2013 A.8.2.1<br>NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6           |
|                         |                                                                                                                                                                                                                                                                                             | <b>ID.AM-6:</b> Cybersecurity roles and responsibilities for the entire workforce and                                                                                   | CIS CSC 17, 19<br>COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03                                                                                                                                  |

The NIST CSF is advantageous over many frameworks in that it is extremely flexible and adaptable to the organisation's specific requirements [20]. A drawback of this is that its Framework Core has only brief guidance the topics - for example, in Table 2, subcategory ID.AM-3 states only, "Organisational communication and data flows are mapped." The framework provides informative references to other frameworks providing further detail.

As discussed by multiple sources [21]–[23], the NIST CSF contains little guidance for cost-benefit analyses when an organisation decides on its target implementation tier, and thus security level.

The framework is relatively new, its initial version released in 2014, and the current revision (V1.1) was released in 2018. This indicates that it is an up-to-date framework, which is especially important to keep up with evolving cybersecurity threats. This has the disadvantage that it has had less time to develop and mature, compared to other frameworks.

The NIST CSF has no official compliance assessment or certification [24], [25] – instead, it is aimed at use in self-assessment. This is a drawback of the framework as it cannot be used by organisations to showcase their reputability, or to prove that they have a well-established security framework. The NIST CSF is advantageous, however, as the documentation is publicly available at no charge.

## 2.3. ISO/IEC 27000 Series

The ISO/IEC 27000 (referred to by number only hereafter) is a series of standards developed jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is one of the most widely adopted security standards. The most relevant documents in the 27000 series to this research are:

- 27000:2018 [4]: Overview and vocabulary
- 27001:2013 [26]: Requirements
- 27002:2013 [27]: Code of practice for information security controls

The 27000 document is an overview of the series. 27001 is the central 27000 standard and contains implementation requirements for an ISMS. 27002 is a complementary standard, which provides more detail on information security controls. These controls are discussed briefly in Annex A of 27001, with 27002 providing more comprehensive information [28], [29]. Examples of the levels of control detail for 27001 and 27002 are shown in Figures 1 and 2, respectively. The level of detail of 27001's Annex A (example shown in Figure 1) is similar to the NIST CSF's Framework Core. 27002 is advantageous in that it gives the 27000 series far more detailed guidance than the NIST CSF, while being flexible in that organisations should only implement 27002 controls to the extent they deem relevant [28], [30].

Of particular importance, 27001 is the only standard in the 27000 series which is audited and certified against [28].

|         |                          |                                                                                       |
|---------|--------------------------|---------------------------------------------------------------------------------------|
| A.6.1.3 | Contact with authorities | <i>Control</i><br>Appropriate contacts with relevant authorities shall be maintained. |
|---------|--------------------------|---------------------------------------------------------------------------------------|

Figure 1: 27001 brief control measure example [26]

### 6.1.3 Contact with authorities

#### Control

Appropriate contacts with relevant authorities should be maintained.

#### Implementation guidance

Organizations should have procedures in place that specify when and by whom authorities (e.g. law enforcement, regulatory bodies, supervisory authorities) should be contacted and how identified information security incidents should be reported in a timely manner (e.g. if it is suspected that laws may have been broken).

#### Other information

Organizations under attack from the Internet may need authorities to take action against the attack source.

Maintaining such contacts may be a requirement to support information security incident management (see [Clause 16](#)) or the business continuity and contingency planning process (see [Clause 17](#)). Contacts with regulatory bodies are also useful to anticipate and prepare for upcoming changes in laws or regulations, which have to be implemented by the organization. Contacts with other authorities include utilities, emergency services, electricity suppliers and health and safety, e.g. fire departments (in connection with business continuity), telecommunication providers (in connection with line routing and availability) and water suppliers (in connection with cooling facilities for equipment).

Figure 2: 27002 detailed control measure example [27, p. 5]

Along with the clauses in the body of the document, 27001/27002 contain 14 clauses, numbered 5 – 18 (shown in Table 3), each with sub-clauses and controls to implement them.

Table 3: 27001/27002 clauses

| Clause number | Clause title                                                   |
|---------------|----------------------------------------------------------------|
| A.5           | Management direction for information security                  |
| A.6           | Organization of information security                           |
| A.7           | Human resource security                                        |
| A.8           | Asset management                                               |
| A.9           | Access control                                                 |
| A.10          | Cryptography                                                   |
| A.11          | Physical and environmental security                            |
| A.12          | Operations security                                            |
| A.13          | Communications security                                        |
| A.14          | System acquisition, development and maintenance                |
| A.15          | Supplier relationships                                         |
| A.16          | Information security incident management                       |
| A.17          | Information security aspects of business continuity management |
| A.18          | Compliance                                                     |

One particularly important clause of the 27001/27002 is compliance, which is scarcely discussed in the NIST CSF [23]. Like the NIST CSF, the 27000 series can be applied to a wide range of organisations, and is broad enough to be implementable in any size organisation [28]. Despite this, the NIST CSF is particularly suited to technology-oriented organisations due to its emphasis on log analytics, incident analytics and technical controls [25].

The 27000 series is advantageous over the NIST CSF in that it is a long-recognised series of standards, implemented more widely in industry, and therefore recognised [25], [29], [31]. The NIST CSF is more up to date than much of the 27000 series – the NIST CSF version 1.1 was released in 2018, while many 2700 series documents are older than this. For example, the newest versions of 27001 and 27002 are from 2013. This has significance due to the importance of maintaining up-to-date standards, as discussed in Section 2.1.

A disadvantage of the 27000 series is that much of the documentation is not available freely, unlike the NIST CSF. This is somewhat counteracted by the certification available for organisations against 27000, allowing them to demonstrate to clients and stakeholders that they implement comprehensive data security measures [25], [32].

## **2.4. IASME Governance Standard for Information and Cyber Security**

The Information Assurance for Small and Medium Enterprises Governance (IASME) Governance Standard for Information and Cyber Security (“IASME Standard”) [33] was introduced in 2011. Its latest version is Revision 5, released in 2018, which is beneficial as it is more current than many frameworks. It includes key security aspects such as incident response, staff training, planning and operation, and is a risk-based framework [34], [35], much like the NIST CSF. The standard describes itself as a catalogue of good practices for increasing the likelihood of an organisation meeting their objectives [33, p. 15]. The standard was developed through a UK Government funded project, aiming to develop an affordable alternative to the 27001 framework for Small and Medium-sized Enterprises (SMEs) [36].

Sections 6 – 9 of the IASME Governance Standard detail the framework’s core principles, which are:

- Identify
- Protect
- Detect and Deter
- Respond and Recover

The IASME Governance Standard describes what is required to meet each core category in its “business information security overview” table [33, p. 19]. Though only containing four key principles, each has sub-sections detailing further requirements (summarised in Table 4). The IASME Standard is helpful in that it contains “Guidance,” “Requirements,” and “Typical questions and performance indicators” subsections for each area.

The IASME Standard achieves deep coverage, like the 27000 series, while remaining very flexible like the NIST CSF [37], [38]. As a result, the standard is suitable for any organisation, and SMEs in particular, while being adjusted for compatibility with other frameworks [33, p. 10], [37].

Table 4: IASME Governance Standard categories

|                               |                                                                                            |
|-------------------------------|--------------------------------------------------------------------------------------------|
| <b>6. Identify</b>            | <b>6.1. Planning</b>                                                                       |
|                               | <b>6.2. Organisation</b>                                                                   |
|                               | <b>6.3. Assets</b>                                                                         |
|                               | <b>6.4. Assessing risks</b>                                                                |
|                               | <b>6.5. Legal and regulatory landscape</b>                                                 |
|                               | <b>6.6. People</b>                                                                         |
| <b>7. Protect</b>             | <b>7.1. Policy realisation</b>                                                             |
|                               | <b>7.2. Physical and environmental protection</b>                                          |
|                               | <b>7.3. Secure business operations</b>                                                     |
|                               | <b>7.4. Assess control</b>                                                                 |
| <b>8. Detect and Deter</b>    | <b>8.1. Malware and technical intrusion</b>                                                |
|                               | <b>8.2. Monitoring, review, and change - for healthy systems and unauthorised activity</b> |
| <b>9. Respond and Recover</b> | <b>9.1. Backup and restore</b>                                                             |
|                               | <b>9.2. Incident management</b>                                                            |
|                               | <b>9.3. Business continuity, disaster recovery, and resilience</b>                         |

The IASME Standard and NIST CSF share categories, both identifying common areas of focus. Category mappings are shown in Table 5.

Table 5: IASME and NIST framework mappings

| <b>IASME to NIST Category Mapping</b> |                                          |
|---------------------------------------|------------------------------------------|
| <b>IASME Governance Standard</b>      | <b>NIST Cybersecurity Framework</b>      |
| <b>6. Identify</b>                    | <b>ID. Identify</b>                      |
| <b>7. Protect</b>                     | <b>PR. Protect</b>                       |
| <b>8. Detect and Deter</b>            | <b>DE. Detect</b>                        |
| <b>9. Respond and Recover</b>         | <b>RS. Respond</b><br><b>RC. Recover</b> |

Despite the similarities in category names, the two frameworks implement them differently, with different subcategories and approaches [38]. For example, the IASME Standard's "Protect" category has a greater emphasis on physical security, and less on training. The IASME Standard's categories and controls are far more technically oriented than the NIST CSF's [39]. Compared to the 27001/27002 clauses, the IASME standard describes many similar areas, although it is more open to adaptation than the 27000 series [37].

The IASME Standard features a risk profile system, implemented similarly to the NIST CSF's framework profiles. The risk profile tiers are Low, Intermediate, and Complex, and are detailed further in Table 6.

Table 6: IASME Governance Framework risk profiles [33, p. 16]

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Low</b>          | The footprint of the organisation's business is small enough to present a small attack surface. The compromise of confidentiality, integrity, and availability would have low impact results because of the relatively low value information assets. Threat agents may not be greatly motivated, resourced, or persistent.                                                                                                                         |
| <b>Intermediate</b> | The footprint of the organisation's business has a significant number of associational paths but not enough to lead inevitably to high-impact compromise of information (at least in part because the relative value of the information is not high). Threat agents are likely to be tailored and targeted to specific information assets to loss of confidentiality, integrity, and availability.                                                 |
| <b>Complex</b>      | The footprint of the organisation's business is a sufficiently sized surface as to risk vulnerabilities to the information handled with high impact results if compromised. The information held by the organisation will have particular sensitivity for it or its customers. Threat agents are likely to be well resourced and sufficiently motivated to make persistent efforts to exfiltrate data and reduce or suspend operational integrity. |

Like the NIST CSF, the IASME Standard is advantageous over the 27000 series as its documentation is freely available – making it more accessible. However, it is beneficial over the NIST CSF due to its certification, allowing organisations to be recognised for their security measures. The certification is aligned with the 27001 certification [34], [37] and is based on an on-site audit after completing a self-assessment [33], [34]. It is also far more affordable than the 27001 certification, costing only £400 + VAT [34], compared to the IT Governance website's estimated cost of 27001 certification of £2,850 - £14,250, based on organisation size [40].

## 2.5. CIS Controls Framework

Initially published by the SysAdmin, Audit, Network, and Security (SANS) Institute in 2008 [41], [42], the framework was known as “(Top) 20 Critical Security Controls” [41], [43]. Ownership has since been transferred to the Centre for Internet Security (CIS), who renamed the framework the CIS Controls (“CIS Framework”). The CIS Framework’s current version is 7.1, released in 2019 [44]. As with the IASME Standard and NIST CSF, this is advantageous as it remains up to date with evolving technology and threats. The framework comprises primarily of the controls document [44], with an accompanying implementation guide [45].

The CIS Framework provides 20 controls. Each control is described in detail along with providing specific sub-controls [46] (example shown Table 7). The CIS Framework features “implementation groups,” which function similarly to the NIST CSF’s profiles, and the IASME Standard’s risk profiles. The implementation groups are labelled 1, 2 and 3, depending on the scale of the organisation, detailed in Table 8. The CIS Framework is beneficial in that it aligns its three implementation groups with each control and its sub-controls. This makes it clearer for those implementing the controls to understand which ones are relevant to their organisation. It is also beneficial in that the CIS provides additional documentation for applying the controls to specific niches, such as Internet of Things (IoT) [47] and the cloud [48].

Table 7: CIS Framework control example [44, p. 22]

| <b>CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers</b> |                   |                          |                                                      |                                                                                                                                                                                                                                                                    |                                                                                       |                                                                                       |                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------|-------------------|--------------------------|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <b>Sub-Control</b>                                                                                                         | <b>Asset Type</b> | <b>Security Function</b> | <b>Control Title</b>                                 | <b>Control Descriptions</b>                                                                                                                                                                                                                                        | <b>Implementation Groups</b>                                                          |                                                                                       |                                                                                       |
|                                                                                                                            |                   |                          |                                                      |                                                                                                                                                                                                                                                                    | <b>1</b>                                                                              | <b>2</b>                                                                              | <b>3</b>                                                                              |
| 5.1                                                                                                                        | Applications      | Protect                  | Establish Secure Configurations                      | Maintain documented security configuration standards for all authorized operating systems and software.                                                                                                                                                            |  |  |  |
| 5.2                                                                                                                        | Applications      | Protect                  | Maintain Secure Images                               | Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates. |                                                                                       |  |  |
| 5.3                                                                                                                        | Applications      | Protect                  | Securely Store Master Images                         | Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.                                                                                |                                                                                       |  |  |
| 5.4                                                                                                                        | Applications      | Protect                  | Deploy System Configuration Management Tools         | Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.                                                                                                      |                                                                                       |  |  |
| 5.5                                                                                                                        | Applications      | Detect                   | Implement Automated Configuration Monitoring Systems | Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.                                             |                                                                                       |  |  |

Table 8: CIS Framework implementation groups [44, p. 5]

|  | Definitions                                                                                                                                                                                                                                    | 1                                                                                   | 2                                                                                   | 3                                                                                   |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|                                                                                   | CIS Sub-Controls for small, commercial off-the-shelf or home office software environments where sensitivity of the data is low will typically fall under IG1. Remember, any IG1 steps should also be followed by organizations in IG2 and IG3. |  |  |  |
|                                                                                   | CIS Sub-Controls focused on helping security teams manage sensitive client or company information fall under IG2. IG2 steps should also be followed by organizations in IG3.                                                                   |                                                                                     |  |  |
|                                                                                   | CIS Sub-Controls that reduce the impact of zero-day attacks and targeted attacks from sophisticated adversaries typically fall into IG3. IG1 and IG2 organizations may be unable to implement all IG3 Sub-Controls.                            |                                                                                     |                                                                                     |  |

The CIS Framework's controls are categorised as being either Basic, Foundational, or Organisational. The Basic and Organisational categories contain controls which mostly address general management, whereas the Foundational category contains technical controls. The control groups are listed along with their categories in Table 9.

Table 9: CIS controls by category

| Basic                                                                                                  | Foundational                                                                          | Organisational                                          |
|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------|
| 1. Inventory and Control of Hardware Assets                                                            | 7. Email and Web Browser Protections                                                  | 17. Implement a Security Awareness and Training Program |
| 2. Inventory and Control of Software Assets                                                            | 8. Malware Defences                                                                   | 18. Application Software Security                       |
| 3. Continuous Vulnerability Management                                                                 | 9. Limitation and Control of Network Ports, Protocols and Services                    | 19. Incident Response and Management                    |
| 4. Controlled Use of Administrative Privileges                                                         | 10. Data Recovery Capabilities                                                        | 20. Penetration Tests and Red Team Exercises            |
| 5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers | 11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches |                                                         |
| 6. Maintenance, Monitoring and Analysis of Audit Logs                                                  | 12. Boundary Defence                                                                  |                                                         |
|                                                                                                        | 13. Data Protection                                                                   |                                                         |
|                                                                                                        | 14. Controlled Access Based on the Need to Know                                       |                                                         |
|                                                                                                        | 15. Wireless Access Control                                                           |                                                         |
|                                                                                                        | 16. Account Monitoring and Control                                                    |                                                         |

As discussed by S. Groš [43] and V. Venkatesh [49], the key difference between the CIS Framework and the other evaluated frameworks is that it has already made risk-based decisions on behalf of organisations. Although it recommends performing a risk assessment [44, p. 4], many of its controls assume the outcomes of such a risk assessment. This approach reduces the flexibility of the framework.

Similar to the IASME Standard, the CIS Framework consists of mostly technical controls [43], [49], [50]. However, the CIS Framework also contains some business and management controls, combining the benefits of technical and management approaches. A drawback of the CIS Framework is that many of its controls are not suitable for automation [42], [46]. Its controls are more flexible than 27000's controls, although they are less extensive.

Like the NIST CSF and IASME Standard, the CIS Framework and its supporting documents are freely available. However, a drawback of this framework is that it has no certification. Certification is only available against the CIS benchmarks – a series of environment-specific benchmarks based loosely on the CIS Controls [51].

### 3. Security Framework Design (Task 2)

A custom security framework was developed based on the most appropriate aspects of the reviewed frameworks in Section 2, and on core understanding of the field gained through lectures and research. The framework was developed for the assignment case scenario, while retaining flexibility. This section describes the framework along with the influence the frameworks literature review (Section 2) had on it.

#### 3.1. Framework Design Influences

The Developed Framework (TDF) combines the strengths of the four reviewed frameworks, along with providing guidance on topics which were overlooked by them. TDF consists of six core categories:

- Identify
- Educate
- Implement
- Review
- Preserve
- Recover

Category 1. Identify was largely influenced by the Identify sections of the NIST CSF and IASME Standard. 1.1 discusses identifying a desired security level – an approach borrowed from the “Implementation Group / Tier / Profile” feature shared by NIST CSF, IASME Standard, and CIS Framework. TDF 1.2 is derived from NIST CSF category ID.RA and IASME 6.4. TDF 1.3’s emphasis on assessing the need for training was derived from IASME section 6.6 and NIST CSF subcategory PR.AT.

TDF’s Category 2. Educate was designed based on factors discussed in the previous paragraph. Additionally, the need for training in specific topics, and assessing staff (TDF 2.1 and 2.2 respectively), were determined based on the CIS Framework controls 17.1 – 17.4.

Category 3. Implement of TDF was informed primarily by research into the field, identifying an area undervalued in the frameworks reviewed, though TDF 3.1’s discussion on physical security was inspired by the 27000 series’ emphasis on it. Additionally, TDF 3.3’s detail of policy implementation was inspired by controls 17 and 18 of the CIS Framework, subcategory ID.GV-1 of the NIST CSF, and section 7.1 of the IASME Standard.

TDF’s Category 4. Review was based on broad discussion of the security review process throughout the frameworks reviewed. 4.1’s requirements for audits and compliance were inspired by 27002’s sections 12.7, and 18, respectively. TDF 4.2 and 4.3 discuss self-assessment and self-improvement, in line with the NIST CSF’s general discussion of self-assessment.

TDF Category 5. Preserve is based on general discussion of the need to maintain processes and policies throughout the CIS Framework, and NIST CSF subcategory PR.IP. TDF 5.1 and 5.2 discuss the need to update security measures, policies, and implementation of the framework itself, in line with NIST CSF subcategory RS.IM and 27002 section 7.2.2.

Category 6. Recover of TDF has been influenced by IASME Standard's section 9 and NIST CSF category RC – Recover. TDF 6.1 and 6.3 are influenced by the same policy requirements as discussed previously, with 6.3 emphasising self-improvement as in the NIST CSF. TDF 6.2 is influenced by IASME Standard section 9.3's discussion of retaining "business as usual" throughout recovery where possible.

### **3.2. Case Scenario Relevance**

Framework design was also influenced by academic articles discussing framework design [52]–[57], particularly BYOD frameworks [58]–[62] as the case scenario implies the necessity of a BYOD approach:

*"...allow staff and customers to use their personal devices to access the company's network/resources".*

The case scenario discusses the high proportion of wireless communications within its network. As such, the framework focused especially on both implementing and reviewing security measures, due to the increased vulnerability of wireless networks over wired ones.

Also discussed in the case scenario is the company's reliance on cloud services. This affected the framework broadly, though particularly influencing the framework's discussion of contingency planning, mitigation, and recovery methods, due to the reliance on external services. This also affected the inclusion of compliance in the framework, due to the handling of data by third parties.

Finally, the case scenario details the vast online presence, particularly on social media. This factor, along with previously discussed areas, influenced the framework's focus on education, training, and assessment. For example, training to identify and handle social engineering attacks.

### 3.3. Framework Resources for CaribbeanCoffee

The framework core is shown in Table 10, including sub-categories / controls, and guidance for each of these. The specificity and scope of each of the six categories are represented as an hourglass in Figure 3, followed by the framework's hierarchy in Figure 4. The order of implementation of TDF is provided in Figure 5. Where possible, these resources use layman's terms, making them readable to anyone in an organisation, but also technical enough to be useful to IT and InfoSec staff.



Figure 3: Proposed framework specificity and scope

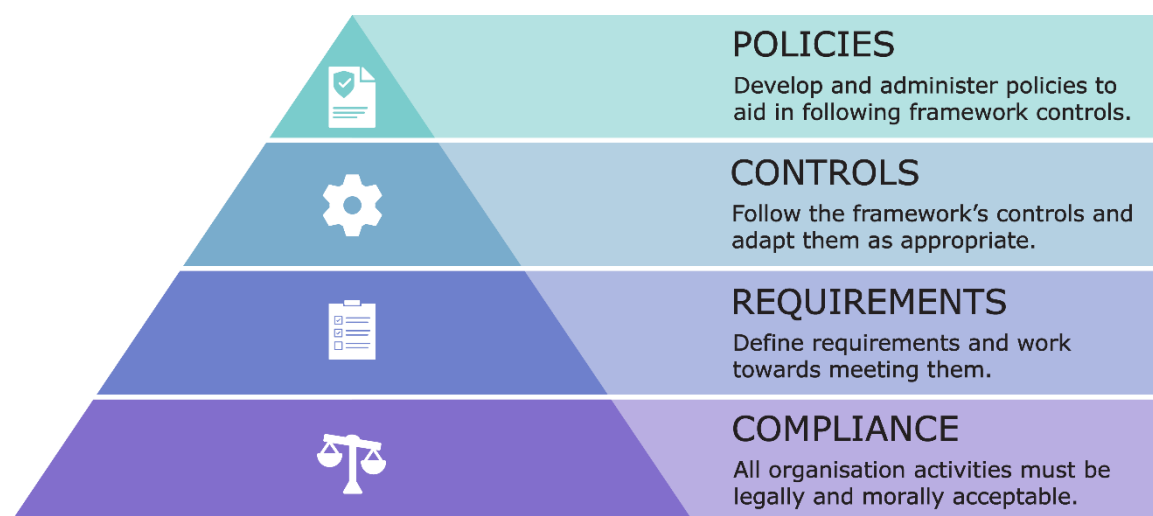


Figure 4: Proposed framework hierarchy

Table 10: Framework Core

| Framework V1.0 |                                                                                                                               |                                                                                                                                                                                                                           |
|----------------|-------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Category       | Subcategory                                                                                                                   | Notes                                                                                                                                                                                                                     |
| 1. IDENTIFY    | 1.1. Identify desired security level, and requirements to meet it.                                                            | The organisation should decide to what level and extent of security they need.                                                                                                                                            |
|                | 1.2. Identify potential risks and protection mechanisms, including policies (including cost-benefit analysis if appropriate). | E.g. identifying phishing as a threat, and education + email scanning software as protection. Risk matrices could be beneficial.                                                                                          |
|                | 1.3. Identify level of training / education for various staff groups.                                                         | Different roles may require varying awareness - identify the level required by each role.                                                                                                                                 |
| 2. EDUCATE     | 2.1. Educate staff on a topic-by-topic basis.                                                                                 | Educating could incorporate workshops, formal classes, or e-learning. The areas to educate and assess will be dependent on the result of 1.3. Assessing could be internal, or use external accreditation / certification. |
|                | 2.2. Assess staff understanding and competency.                                                                               |                                                                                                                                                                                                                           |
|                | 2.3. Update teaching and assessing regularly to adapt to changing circumstances, new technologies and threats, etc.           | This could consist of updating the teaching method, or the content - avoid educating staff on outdated information.                                                                                                       |
| 3. IMPLEMENT   | 3.1. Implement physical security.                                                                                             | Implement both physical and information security in tandem to the extent identified in 1.1. This will likely benefit from any educating and training undertaken during 2.1.                                               |
|                | 3.2. Implement cyber / information security.                                                                                  |                                                                                                                                                                                                                           |
|                | 3.3. Implement policies as necessary and ensure they are accessible to all (language, braille, readability etc.).             | Implement policies as identified in 1.2. Some examples are email, password, and Bring Your Own Device (BYOD) policies.                                                                                                    |
| 4. REVIEW      | 4.1. Conduct Internal and / or external audits for compliance. Thoroughly review legal and ethical concerns.                  | Regular reviews (timeframe decided by organisation) against the initial requirements. Document the organisation's compliance against the framework and the processes put into place to achieve compliance.                |
|                | 4.2. Conduct organisation self-assessment against initial security requirements from 1.1 and 1.2.                             |                                                                                                                                                                                                                           |
|                | 4.3. Learn from difficulties and issues. If necessary, return to 3, or even 1.1. if necessary.                                | Reflect on gaps or difficulties in security and refine by returning to steps 3.1 - 3.3, then reviewing again.                                                                                                             |
| 5. PRESERVE    | 5.1. Preserve data integrity by maintaining the current procedures long-term, and renew hardware and software.                | Ensure that procedures are maintained. Train new staff on joining the organisation, or when staff roles change.                                                                                                           |
|                | 5.2. Update security measures - remain up to date with organisation scope, technology use, and threats.                       | E.g. if the organisation decides to adopt BYOD or similar, new measures should be put in place.                                                                                                                           |
|                | 5.3. Update policies and implementation of <b>this framework</b> as necessary to adapt to the organisation's changing needs.  | Remain up to date with advancements in technology, threats, and usage of technology - this should be reflected in policies.                                                                                               |
| 6. RECOVER     | 6.1. Implement contingency plans and revert to backups in line with policies.                                                 | Adopt a "business as usual" approach to productivity during recovery, where possible.                                                                                                                                     |
|                | 6.2. Maintain operations and business image.                                                                                  | Maintain stakeholder and client impressions of the organisation.                                                                                                                                                          |
|                | 6.3. Update and improve recovery procedures to adapt to new systems, and learn from past recoveries.                          | Adapt recovery procedures in line with changes in the organisation.                                                                                                                                                       |

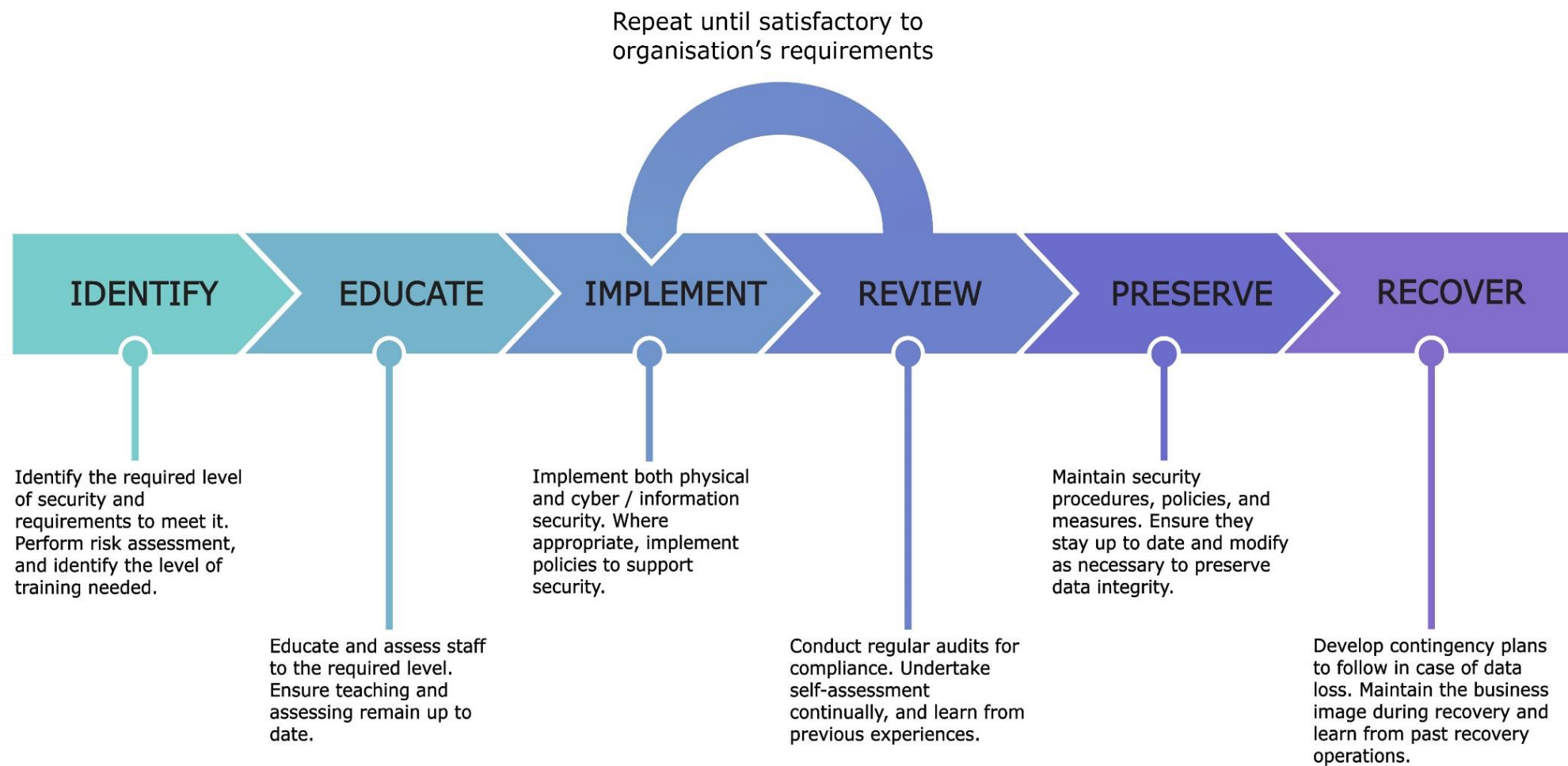


Figure 5: The developed framework order of implementation

## **4. Conclusion and Future Work**

This research has investigated four InfoSec frameworks, and critically analysed and evaluated them. From these findings, a custom framework was developed for the case scenario which adopted the strengths of each of the reviewed frameworks. Framework design was also influenced by background knowledge gained through lectures and research. The primary focuses of the developed framework are to identify, educate, implement, review, preserve, and recover, each with their own sub-categories.

Framework design was successful, being both specific to the case scenario, and broad and adaptable to other scenarios. Future work could entail developing more detailed guidance for each sub-category, such as specific security implementation guidance and required training areas. It could also include a review of a wider range of frameworks to further support framework design.

## References

- [1] M. E. Whitman and H. J. Mattord, *Management of Information Security*, 6th ed. Boston, MA: Cengage Learning.
- [2] A. Plate, "ISMS: A Management Framework for Information Security," in *Encyclopedia of Cryptography and Security*, H. C. A. van Tilborg and S. Jajodia, Eds. Boston, MA: Springer US, 2011, pp. 647–648.
- [3] Luke Irwin, "What is an ISMS, and why does your organisation need one? - IT Governance Blog En," 2019. <https://www.itgovernance.eu/blog/en/what-is-an-isms-and-why-does-your-organisation-need-one> (accessed Oct. 20, 2020).
- [4] International Organization for Standardization and International Electrotechnical Commission, "ISO/IEC 27000:2018: Information technology — Security techniques — Information security management systems — Overview and vocabulary," 2018.
- [5] Government of the United Kingdom, "Data Protection Act 2018 Chapter 12," 2018. Accessed: Dec. 28, 2018. [Online]. Available: [http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga\\_20180012\\_en.pdf](http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf).
- [6] GOV.UK, "Data protection - GOV.UK," 2018. <https://www.gov.uk/data-protection> (accessed Dec. 28, 2018).
- [7] European Parliament and Council of European Union, "EU General Data Protection Regulation 2016/679," *Off. J. Eur. Union*, 2016.
- [8] Information Commissioner's Office, "Guide to the General Data Protection Regulation (GDPR)," 2018. [Online]. Available: [https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/%0Ahttps://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/%0Ahttps://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf).
- [9] E.-S. M., M. Saber, and R. Arnous, "An Integrated Framework to Ensure Information Security Over the Internet," *Int. J. Comput. Appl.*, vol. 178, no. 29, pp. 13–15, 2019, doi: 10.5120/ijca2019919117.
- [10] N. Miloslavskaya and A. Tolstoy, "Internet of Things: information security challenges and solutions," *Cluster Comput.*, vol. 22, no. 1, pp. 103–119, 2019, doi: 10.1007/s10586-018-2823-6.
- [11] D. Taneja and S. S. Tyagi, "Information Security in Cloud Computing: A systematic Literature Review and Analysis," *Int. J. Sci. Eng. Technol.*, vol. 6, no. 1, pp. 50–55, 2017, doi: 10.17950/ijset/v6s1/110.
- [12] T. McGill and N. Thompson, "Old risks, new challenges: exploring differences in security between home computer and mobile device use," *Behav. Inf. Technol.*, vol. 36, no. 11, pp. 1111–1124, 2017, doi: 10.1080/0144929X.2017.1352028.
- [13] A. Hovav and F. F. Putri, "This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy," *Pervasive Mob. Comput.*, vol. 32, pp. 35–49, 2016, doi: 10.1016/j.pmcj.2016.06.007.

- [14] M. Olalere, M. Taufik Abdullah, R. Mahmud, and A. Abdullah, "Bring Your Own Device: Security Challenges and A theoretical Framework for Two-Factor Authentication," *Int. J. Comput. Networks Commun. Secur.*, vol. 4, no. 1, pp. 21–32, 2016, [Online]. Available: [www.ijcnscs.org](http://www.ijcnscs.org).
- [15] M. Cooney, "UPDATE 4-28 : How enterprise networking is changing with a work-at-home workforce," *Netw. World*, 2020, [Online]. Available: <https://search-proquest-com.tarcez.tarc.edu.my/docview/2395349628?accountid=38945%0A>.
- [16] A. Calder, *NIST Cybersecurity Framework: A pocket guide*. Ely, Cambridgeshire: IT Governance Publishing, 2018.
- [17] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1," 2018.
- [18] A. Ibrahim, C. Valli, I. McAteer, and J. Chaudhry, "A security review of local government using NIST CSF: a case study," *J. Supercomput.*, vol. 74, no. 10, pp. 5171–5186, 2018, doi: 10.1007/s11227-018-2479-2.
- [19] M. Orolet, "Learn What NIST's Cybersecurity Framework Can Do For You," *Netw. World*, no. Jun, pp. 1–3, 2017, [Online]. Available: <http://www.csoonline.com/article/3199968/network-security/learn-what-nists-cybersecurity-framework-can-do-for-you.html>.
- [20] A. Gabriel, J. Shi, and C. Ozansoy, "A Proposed Alignment of the National Institute of Standards and Technology Framework with the Funnel Risk Graph Method," *IEEE Access*, vol. 5, no. June 2017, pp. 12103–12113, 2017, doi: 10.1109/ACCESS.2017.2718568.
- [21] I. Lee, "Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management," *Futur. Internet*, vol. 12, no. 9, pp. 157–178, 2020, doi: 10.3390/fi12090157.
- [22] L. A. Gordon, M. P. Loeb, and L. Zhou, "Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model," *J. Cybersecurity*, vol. 6, no. 1, pp. 1–8, 2020, doi: 10.1093/cybsec/tyaa005.
- [23] S. Almuhammadi and M. Alsaleh, "Information Security Maturity Model for Nist Cyber Security Framework," in *Conference: Sixth International Conference on Information Technology Convergence and Services*, 2017, no. February 2017, pp. 51–62, doi: 10.5121/csit.2017.70305.
- [24] N. Teodoro, L. Gonçalves, and C. Serrão, "NIST cybersecurity framework compliance: A generic model for dynamic assessment and predictive requirements," in *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, 2015, vol. 1, pp. 418–425, doi: 10.1109/Trustcom.2015.402.
- [25] P. P. Roy, "A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard," in *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications, NCETSTE*, 2020, pp. 1–3, doi: 10.1109/NCETSTE48365.2020.9119914.

- [26] International Organization for Standardization and International Electrotechnical Commission, "ISO/IEC 27001:2013: Information Technology - Security Techniques - Information Security Management Systems - Requirements," 2013.
- [27] International Organization for Standardization and International Electrotechnical Commission, "ISO/IEC 27002:2013: Information technology — Security techniques — Code of practice for information security controls," 2013.
- [28] L. Irwin, "What is the ISO 27000 series of standards? - IT Governance UK Blog," 2019. <https://www.itgovernance.co.uk/blog/what-is-the-iso-27000-series-of-standards> (accessed Oct. 13, 2020).
- [29] R. Leszczyna, "A review of standards with cybersecurity requirements for smart grid," *Comput. Secur.*, vol. 77, pp. 262–276, 2018, doi: 10.1016/j.cose.2018.03.011.
- [30] S. Cha, S. Baek, S. Kang, and S. Kim, "Security Evaluation Framework for Military IoT Devices," *Secur. Commun. Networks*, vol. 2018, 2018, doi: 10.1155/2018/6135845.
- [31] R. Leszczyna, "Standards with cybersecurity controls for smart grid—A systematic analysis," *Int. J. Commun. Syst.*, vol. 32, no. 6, pp. 1–20, 2019, doi: 10.1002/dac.3910.
- [32] A. Calder, "Certification Process," in *ISO27001/ISO27002 a Pocket Guide*, 2nd ed., Cambridgeshire: IT Governance Publishing, 2013, pp. 13–15.
- [33] D. G. Dresner, "The IASME governance standard for information and cyber security. Issue 5.0.," 2018. [Online]. Available: <https://iasme.co.uk/wp-content/uploads/2019/04/IASMEStandardv5.pdf>.
- [34] IASME Consortium Ltd, "IASME Governance | iasme." <https://iasme.co.uk/iasme-governance/> (accessed Oct. 15, 2020).
- [35] R. Henson and D. Sutcliffe, "An Insurance-based Approach to Improving SME Cyber Security," *Spec. Top. Econ. Manag. An Introd.*, pp. 171–186, 2017.
- [36] IASME Consortium Ltd, "About | iasme." <https://iasme.co.uk/about/> (accessed Oct. 16, 2020).
- [37] R. G. Utomo, R. J. Walters, and G. B. Wills, "Factors affecting the implementation of information assurance for eGovernment in Indonesia," in *2017 12th International Conference for Internet Technology and Secured Transactions, ICITST 2017*, 2018, pp. 225–230, doi: 10.23919/ICITST.2017.8356388.
- [38] A. Dedeke and K. Masterson, "Contrasting cybersecurity implementation frameworks (CIF) from three countries," *Inf. Comput. Secur.*, vol. 27, no. 3, pp. 373–392, 2019, doi: 10.1108/ICS-10-2018-0122.
- [39] L. Dalley and E. Apeh, "An Approach for Social Engineering Threat Assessment and Remediation for SMEs," Bournemouth, United Kingdom, 2020.

- [40] IT Governance Ltd, "Typical ISO 27001 certification costs," 2020. <https://www.itgovernance.co.uk/iso27001-certification-costs> (accessed Oct. 17, 2020).
- [41] SANS Institute, "SANS Institute - CIS Critical Security Controls: A Brief History," 2020. <https://www.sans.org/critical-security-controls/history> (accessed Oct. 24, 2020).
- [42] M. Ahmed and E. Al-Shaer, "Measures and metrics for the enforcement of critical security controls: A case study of boundary defense," in *HotSoS '19: Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security*, 2019, no. April, doi: 10.1145/3314058.3317730.
- [43] S. Groš, "A Critical View on CIS Controls," 2019.
- [44] Center for Internet Security, "CIS Controls Version 7.1," 2019. [Online]. Available: <https://learn.cisecurity.org/cis-controls-download>.
- [45] Center for Internet Security, "CIS Controls Implementation Guide for Small- and Medium-Sized CIS Controls Implementation Guide for SMEs," 2019. [Online]. Available: <https://www.cisecurity.org/wp-content/uploads/2017/09/CIS-Controls-Guide-for-SMEs.pdf>.
- [46] B. Barnier and P. Kale, "Cybersecurity: the Endgame—Part One," *Edpacs*, vol. 62, no. 3, pp. 1–18, 2020, doi: 10.1080/07366981.2020.1752466.
- [47] Center for Internet Security, *CIS Controls Internet of Things Companion Guide*. 2019.
- [48] Center for Internet Security, "CIS Controls Cloud Companion Guide," 2019. [Online]. Available: <https://www.cisecurity.org/white-papers/cis-controls-cloud-companion-guide/>.
- [49] V. Venkatesh, "Design of Cybersecurity Risk Assessment Tool for Small and Medium Sized Businesses using the NIST Cybersecurity Framework," in *KSU Proceedings on Cybersecurity Education, Research and Practice*, 2019, no. October 2018, pp. 1–10, [Online]. Available: <https://digitalcommons.kennesaw.edu/ccerp/2018/practice/6>.
- [50] O. Giuca, T. M. Popescu, A. M. Popescu, G. Prostean, and D. E. Popescu, "A Survey of Cybersecurity Risk Management Frameworks," in *Soft Computing Applications. SOFA 2018. Advances in Intelligent Systems and Computing*, vol. 1221., Springer, 2020.
- [51] Center for Internet Security, "CIS Certification – Assessment for CIS Benchmark," 2020. <https://www.cisecurity.org/cis-securesuite/pricing-and-categories/product-vendor/cis-benchmark-assessment/> (accessed Oct. 26, 2020).
- [52] B. A. Mozzaquatro, C. Agostinho, D. Goncalves, J. Martins, and R. Jardim-Goncalves, "An ontology-based cybersecurity framework for the internet of things," *Sensors (Switzerland)*, vol. 18, no. 9, 2018, doi: 10.3390/s18093053.

- [53] C. Joshi and U. K. Singh, "Information security risks management framework – A step towards mitigating security risks in university network," *J. Inf. Secur. Appl.*, vol. 35, pp. 128–137, 2017, doi: <https://doi.org/10.1016/j.jisa.2017.06.006>.
- [54] J. Merchan-Lima, F. Astudillo-Salinas, L. Tello-Oquendo, F. Sanchez, G. Lopez-Fonseca, and D. Quiroz, "Information security management frameworks and strategies in higher education institutions: a systematic review," *Ann. Telecommun.*, no. 2020, 2020, doi: 10.1007/s12243-020-00783-2.
- [55] S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, "Information security governance challenges and critical success factors: Systematic review," *Comput. Secur.*, vol. 99, p. 102030, 2020, doi: <https://doi.org/10.1016/j.cose.2020.102030>.
- [56] W. A. Cram, J. G. Proudfoot, and J. D'Arcy, "Organizational information security policies: a review and research framework," *Eur. J. Inf. Syst.*, vol. 26, no. 6, pp. 605–641, 2017, doi: 10.1057/s41303-017-0059-9.
- [57] A. Nasir, R. A. Arshah, M. R. A. Hamid, and S. Fahmy, "An analysis on the dimensions of information security culture concept: A review," *J. Inf. Secur. Appl.*, vol. 44, pp. 12–22, 2019, doi: <https://doi.org/10.1016/j.jisa.2018.11.003>.
- [58] A. Hovav and F. F. Putri, "This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy," *Pervasive Mob. Comput.*, vol. 32, pp. 35–49, 2016, doi: <https://doi.org/10.1016/j.pmcj.2016.06.007>.
- [59] M. Olalere, M. T. Abdullah, R. Mahmod, and A. Abdullah, "Bring your own device: security challenges and a theoretical framework for two-factor authentication," *Int. J. Comput. Networks Commun. Secur.*, vol. 4, no. 1, pp. 21–32, 2016.
- [60] C. Vorakulpipat, S. Sirapaisan, E. Rattanalernusorn, and V. Savangasuk, "A policy-based framework for preserving confidentiality in BYOD environments: A review of information security perspectives," *Security and Communication Networks*, vol. 2017. Hindawi Limited, 2017, doi: 10.1155/2017/2057260.
- [61] N. Zahadat, P. Blessner, T. Blackburn, and B. A. Olson, "BYOD security engineering: A framework and its analysis," *Comput. Secur.*, vol. 55, pp. 81–99, 2015, doi: <https://doi.org/10.1016/j.cose.2015.06.011>.
- [62] B. Ngoqo and S. V. Flowerday, "Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users," *Comput. Secur.*, vol. 53, pp. 132–142, 2015, doi: <https://doi.org/10.1016/j.cose.2015.05.011>.

## Background Reading

A. Chopra and M. Chaudhary, *Implementing an Information Security Management System: Security Management Based on ISO 27001 Guidelines*. Apress, 2020.

C. D. Heitzenrater and A. C. Simpson, "Policy, statistics and questions: Reflections on UK cyber security disclosures," *J. Cybersecurity*, vol. 2, no. 1, pp. 43–56, 2016, doi: 10.1093/cybsec/tyw008.

D. Achmadi, Y. Suryanto, and K. Ramli, "On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center," in *2018 International Workshop on Big Data and Information Security (IWBIS)*, 2018, pp. 149–157, doi: 10.1109/IWBIS.2018.8471700.

E. Baikloy, P. Praneetpolgrang, and N. Jirawichitchai, "Development of cyber resilient capability maturity model for cloud computing services," *TEM J.*, vol. 9, no. 3, pp. 915–923, 2020, doi: 10.18421/TEM93-11.

F. Nel and L. Drevin, "Key elements of an information security culture in organisations," *Inf. Comput. Secur.*, vol. 27, no. 2, pp. 146–164, 2018, doi: 10.1108/ICS-12-2016-0095.

I. A. Tøndel, M. B. Line, and M. G. Jaatun, "Information security incident management: Current practice as reported in the literature," *Comput. Secur.*, vol. 35, no. 2, pp. 42–57, 2018, doi: 10.1016/j.cose.2014.05.003.

Information Commissioner's Office, "Accountability and governance | ICO." <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/> (accessed Oct. 16, 2020).

M. Bada and J. R. C. Nurse, "Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs)," *Inf. Comput. Secur.*, vol. 27, no. 3, pp. 393–410, 2019, doi: 10.1108/ICS-07-2018-0080.

M. Dawson, "Applying a holistic cybersecurity framework for global IT organizations," *Bus. Inf. Rev.*, vol. 35, no. 2, pp. 60–67, 2018, doi: 10.1177/0266382118773624.

M. Nieves, K. Dempsey, and V. Y. Pillitteri, "NIST Special Publication 800-12 Revision 1 - An introduction to information security," *NIST Spec. Publ.*, 2017, [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf>.

M. Swanson, J. Hash, and P. Bowen, "Guide for developing security plans for information technology systems," *NIST Spec. Publ. 800-18 Revis. 1*, vol. 800, no. February, 2006, [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf> <http://cat.inist.fr/?aModele=afficheN&cpsidt=64084>.

M. Tamimi, "Security Review Based on Iso 27000 / Iso 27001 / Iso 27002 Standards : Security Review Based on Iso 27000 / Iso 27001 / Iso 27002 Standards : a Case Study Research," *Int. J. Manag. Appl. Sci.*, vol. 5, no. 8, pp. 120–123, 2019.

R. Sabillon, "A Practical Model to Perform Comprehensive Cybersecurity Audits," *Enfoque UTE*, vol. 9, no. 1, pp. 127–137, 2018.

S. Choi and J. Kwak, "Enhanced SDIoT Security Framework Models," *Int. J. Distrib. Sens. Networks*, vol. 2016, 2016, doi: 10.1155/2016/4807804.

W. Knowles, A. Baron, and T. McGarr, "The simulated security assessment ecosystem: Does penetration testing need standardisation?," *Comput. Secur.*, vol. 62, pp. 296–316, 2016, doi: 10.1016/j.cose.2016.08.002.