



# ACCA7028



Rohan Chavan (2212517)  
UNIVERSITY OF WALES TRINITY SAINT DAVID

## Table of Contents

|                                                                                                                 |   |
|-----------------------------------------------------------------------------------------------------------------|---|
| Introduction .....                                                                                              | 1 |
| ISO 27000.....                                                                                                  | 1 |
| Cloud Controls Matrix (CCM) .....                                                                               | 2 |
| General Data Protection Regulation (GDPR):.....                                                                 | 2 |
| NatureGarden Security and Compliance Policy Suite .....                                                         | 3 |
| Regularly updating NatureGarden's Security and Compliance Policy Suite is crucial for several reasons:<br>..... | 8 |
| References.....                                                                                                 | 9 |

### Introduction

In the ever-evolving landscape of digital technology, the importance of robust information security and data protection practices cannot be overstated. With increasing cyber threats and stringent data privacy regulations, organizations are under constant pressure to safeguard their information assets. This paper delves into three pivotal standards and frameworks in the realm of information security and data protection: ISO 27000 series, the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM), and the General Data Protection Regulation (GDPR). The ISO 27000 series offers a comprehensive framework for managing information security, CSA CCM specifically addresses cloud security, and GDPR sets forth rigorous data privacy regulations. Together, these frameworks provide a holistic approach to securing digital assets and ensuring compliance in a complex regulatory environment.

### ISO 27000

ISO/IEC worked to establish the ISO 27000 set of standards. These rules provide a framework for enterprises to manage the security of assets such as financial information, intellectual property, personnel details, and third-party information. [1] Central to this series is ISO/IEC 27001, which provides a blueprint for an Information Security Management System (ISMS), a systematic approach to managing sensitive company information so that it remains secure. [2]

The ISO 27001 standard lays out specific requirements and a checklist of controls covering areas like risk management, security policy, communications and operations management, human resource security, development and maintenance, physical and environmental security, asset management, access control, information systems acquisition, and compliance. [1]

Implementing ISO 27001 involves a comprehensive process that includes [3]:

- Conducting a risk assessment to identify potential information security threats and vulnerabilities.
- Designing and implementing a comprehensive set of information security controls and other forms of risk management to address identified risks.
- Adopting an overarching management process to ensure that the information security controls continue to meet the organization's evolving information security needs.

The benefits of implementing the ISO 27000 series include demonstrating compliance with legal, regulatory, and contractual requirements, protecting the organization's brand image, and providing a competitive advantage.

#### Cloud Controls Matrix (CCM)

The Cloud Security Alliance is responsible for the development of a cybersecurity control architecture for cloud computing that is known as the Cloud Controls Matrix (CCM). 133 control objectives are included in it, and they are arranged in 17 different domains. These control goals cover all of the essential aspects of cloud technology. Among the most significant contributions to the best practices for cloud security, the Cloud Computing Matrix (CCM) is widely recognised as being among the most essential. [4]

The matrix provides businesses with the necessary structure, detail, and clarity in relation to information security that is suitable for cloud computing. This is accomplished via the use of the matrix tool. Through the use of the information security matrix, this is achieved. The CCM is accountable for ensuring that its controls are consistent with the security standards, rules, and control frameworks that are already in place within the industry. This task falls within the CCM's purview. PCI, NIST, ISO 27001/27002, ISACA COBIT, and NERC CIP are three examples of these kind of standards. [5]

The domains covered in the CCM include application and interface security, audit assurance and compliance, business continuity management and operational resilience, change control and configuration management, data security and information lifecycle management, encryption and key management, governance and risk management, human resources, identity and access management, infrastructure and virtualization security, inter-operability and portability, mobile security, security incident management, legal and compliance, threat and vulnerability management, and universal endpoint management. [4]

The implementation of CCM in an organization involves [6]:

- Assessing the current cloud services against the CCM to identify gaps in existing security practices.
- Developing a roadmap for compliance with the CCM, prioritizing actions based on the identified gaps.
- Regularly reviewing and updating the cloud security practices aligning with the latest version of the CCM.

Adopting CCM helps in enhancing an organization's cloud security posture, ensuring comprehensive risk management in cloud environments, and demonstrating commitment to security best practices in cloud computing. [7]

#### General Data Protection Regulation (GDPR):

Everyone is obligated to comply with the General Data Protection Regulation (GDPR), which is a regulation originating from the European Union that regulates the protection of personal information and its privacy. Any and all individuals who are located inside the borders of the European Union and the European Economic Area are subject to this regulation. Both the simplification of the legal environment for international business and the provision of individuals with control over their personal data are the goals of the General Data Protection Regulation

(GDPR). Within the European Union, the harmonisation of law will be the means by which this objective will be attained. [8]

**Key components of GDPR include [9]:**

- Rights of data subjects, including the right to access, right to be forgotten, right to data portability, and right to object.
- Obligations for data controllers and processors, including requirements for data protection by design and by default, keeping detailed records of data processing activities, and conducting data protection impact assessments.
- Strict consent requirements for processing personal data.
- Data breach notification requirements.

**GDPR compliance involves few of below components [10]:**

- Conducting a data protection impact assessment to identify and mitigate risks.
- Updating data protection policies and procedures, including consent mechanisms.
- Appointing a Data Protection Officer (DPO) if required.
- Implementing and demonstrating compliance with the data protection principles.

GDPR has significantly impacted the way organizations around the world collect, use, and manage personal data, enforcing a higher standard of data protection and privacy.

**Conclusion :** In conclusion, the ISO 27000 series, CSA Cloud Controls Matrix, and GDPR each play a crucial role in shaping the landscape of information security and data privacy. By understanding and implementing these frameworks and regulations, organizations like NatureGarden can not only ensure the protection of their digital assets but also foster a culture of security awareness and compliance. As the digital landscape continues to evolve, staying informed and adaptive to these standards will be key to maintaining robust security and compliance postures in an increasingly interconnected world.

[NatureGarden Security and Compliance Policy Suite](#)

Welcome to the NatureGarden Security and Compliance Policy Suite. In a world where digital technology is rapidly evolving and data security threats are constantly emerging, NatureGarden is committed to safeguarding our information assets, employee's data, intellectual property, and customer trust. Our comprehensive suite of policies is designed to ensure the highest standards of security and compliance across all facets of our operations.

This policy suite encompasses a range of key areas including the use of technology resources, personal device management (BYOD), information security, social media engagement, cloud security, and intellectual property protection. Each policy within this suite has been meticulously developed to align with global best practices, legal standards, and regulatory requirements.

Our aim is to create a secure and responsible work environment that not only protects NatureGarden's assets but also fosters a culture of awareness and accountability among our employees and partners. Adherence to these policies is essential for maintaining the integrity,

confidentiality, and availability of our information systems and for upholding the reputation of NatureGarden as a leader in our industry.

We encourage all employees and stakeholders to familiarize themselves with these policies, as their commitment and cooperation are integral to our collective success in navigating the complexities of the modern digital landscape.

## 1. **Acceptable Use Policy for Technology Resources** [11]

1.1 **Purpose:** To define standards for responsible usage of technology resources to ensure security and compliance.

1.2 **Scope:** Applies to all NatureGarden employees, contractors, and any authorized users.

### 1.3 **Requirements:**

#### **Authorized Equipment Usage:**

- Laptops: Employees required to use laptops provided or approved by the IT department, pre-loaded with necessary security software and configured with access controls.
- Mobile Devices: Implement a Bring Your Own Device (BYOD) policy, Only IT approved mobile devices are acceptable for accessing corporate data and the security measures required (e.g., strong passwords, encryption).
- Removable Media: It is restricted to use of USB drives and other removable media, unless approved by IT and encrypted for data transfer.
- Personal Cloud Storage: Prohibited the use of personal cloud storage platforms for storing or sharing corporate data, directing employees to approved enterprise cloud solutions.

#### **Data Protection:**

- All sensitive data, including customer information, financial records, intellectual property, and trade secrets, must be encrypted at rest and in transit.
- Approved encryption methods and tools will be specified by the IT department.
- Encryption keys must be securely stored and managed.

#### **Strong Password Requirements** [12]:

- At least 12 characters in length
- A combination of uppercase and lowercase letters, numbers, and symbols
- Not based on personal information or common words
- Not reused across multiple accounts
- Passwords must be changed every 3 Months.
- Password managers are strongly encouraged to store and manage passwords securely.

**2FA must be enabled for all user accounts that access sensitive systems or data.**

**Approved 2FA methods include [13]:**

- Time-based one-time passwords (TOTP) apps
- Authenticator apps
- Security keys
- Phone-based text or call verification

**Prohibited Activities:**

**Unauthorized Software Installations [14]:**

- Installing any software not approved by the IT department on company devices, including laptops, mobile phones, and removable media.
- Bypassing or attempting to disable security measures implemented on company systems.
- Downloading or using pirated software.

**Misuse of Passwords and Accounts [15]:**

- Sharing password or account credentials with anyone.
- Using weak or easily guessable passwords.
- Accessing or attempting to access unauthorized systems or data, even if accidentally discovered.
- Engaging in password phishing or cracking attempts.

**Illegal Activities [16]:**

- Using company resources to engage in any illegal activity, including downloading or viewing illegal content, accessing unauthorized websites, or violating copyright laws.
- Sending or receiving harassing, discriminatory, or offensive content through company systems.
- Using company resources for personal gain that is not approved or conflicts with company interests.

**Unauthorized Sharing of Sensitive Information [17]:**

- Disclosing confidential company information or customer data to any unauthorized individuals or entities.
- Uploading or storing sensitive data on unauthorized cloud storage platforms or personal devices.
- Sending or receiving sensitive information through unapproved channels or applications.

**Additional Prohibited Actions [18]:**

- Tampering with or damaging company hardware or software.

- Defacing or vandalizing company systems or data.
- Misusing company resources for personal activities during work hours beyond reasonable breaks.
- Failing to report any suspected security incidents or potential threats.

#### **Responsible Internet Usage [19]:**

##### **DO:**

- Use only for approved work tasks and professional communication.
- Maintain professional conduct and language online.
- Follow security protocols like strong passwords and MFA.
- Report suspicious activity or potential threats.

##### **DON'T:**

- Access pirated or illegal content.
- Engage in personal activities during work hours.
- Share confidential information on unauthorized platforms.
- Click on suspicious links or download unauthorized software.

## **2. Bring Your Own Device (BYOD) Policy [20]**

**2.1 Purpose:** To enable secure and efficient use of personal devices for work-related activities.

**2.2 Scope:** All employees using personal devices for work.

### **2.3 Requirements:**

- **Device Registration:** All personal devices must be registered with the IT department for security vetting and compatibility checks.
- **Security Measures:** Mandatory installation of approved security software, encryption of stored data, and adherence to security updates.
- **Data Segregation:** Clear guidelines on separating personal and work data, possibly through containerization or virtualization techniques.
- **Incident Reporting:** Immediate reporting protocols for any security incidents or device loss/theft.

## **3. Information Security Policy [21]**

**3.1 Purpose:** To establish a comprehensive framework for securing information assets.

**3.2 Scope:** Encompasses all information security aspects including digital, physical, and personnel security.

3.3 **Key Principles:** Confidentiality, integrity, availability, and accountability.

3.4 **Key Procedures:**

- Regular, detailed risk assessments to identify potential threats.
  - Access control based on the least privilege principle.
  - Comprehensive incident response procedures for various scenarios.
  - Adherence to data privacy laws and industry standards.
  - Bi-annual security awareness training for all employees.
- 3.5 **Enforcement:** Strict enforcement measures, including potential legal action for non-compliance.

#### 4. **Social Media Policy** [22]

4.1 **Purpose:** Guide responsible use of social media platforms.

4.2 **Scope:** All NatureGarden representatives using social media for work.

4.3 **Requirements:**

- **Representation and Transparency:** Guidelines on how to represent NatureGarden and disclose affiliations.
  - **Content Accuracy and Professionalism:** Standards for ensuring information accuracy, respecting copyright, and maintaining professionalism.
  - **Confidentiality:** Prohibition of sharing confidential or proprietary information.
- 4.4 **Enforcement:** Violations lead to actions ranging from warnings to employment termination.

#### 5. **Cloud Security Policy** [23]

5.1 **Purpose:** Ensure the secure use of cloud services.

5.2 **Scope:** All cloud-based operations and data storage.

5.3 **Requirements:**

- **Approved Providers:** Use of vetted cloud service providers adhering to industry-standard security practices.
- **Data Handling:** Specific protocols for data encryption, transfer, and storage.
- **Access Management:** Robust access controls and regular reviews.
- **Monitoring and Compliance:** Continuous monitoring for anomalies, regular compliance audits.
- **Enforcement:** Violations will result in access restrictions or further disciplinary actions.

#### 6. **Intellectual Property Protection Policy** [24]

6.1 **Purpose:** Safeguard NatureGarden's intellectual assets.

6.2 **Scope:** All individuals involved with NatureGarden's IP.

### 6.3 Principles:

- **Be an "IP Insider":** We have amazing inventions, trademarks, and trade secrets – things that give us a competitive edge. Understanding what this IP is and how it's protected will make you a true NatureGarden hero. Keep an eye out for training sessions and resources that'll make you an IP expert!
- **Zip it, lock it, NDA it:** Our trade secrets are the crown jewels of the garden. Keep them under wraps! Don't share confidential information with anyone outside the company, unless they've signed a Non-Disclosure Agreement (NDA). Remember, even casual chatter can be harmful.
- **Report suspicious activity:** Think you've spotted someone trying to pick the lock on our IP garden? Don't hesitate to report it! We have dedicated channels for any concerns you might have, and speaking up could protect our innovations from potential threats.
- **Let's work together:** Protecting our IP is a team effort. This policy isn't just a set of rules – it's a roadmap for collaboration. If you have questions, suggestions, or anything else on your mind, reach out to your manager or the IP team.

## 7. Consequences of Policy Violation in NatureGarden Security and Compliance Policy Suite

At NatureGarden, compliance with our Security and Compliance Policy Suite is crucial. Violations are taken seriously and result in consequences based on the infraction's severity. Minor offenses may lead to warnings and educational counselling. Significant breaches can invoke disciplinary actions, including suspension, demotion, or financial penalties, as per NatureGarden's HR guidelines.

Severe violations, especially those involving malicious intent or substantial harm to the company or its clients, could result in termination and potential legal proceedings. Every incident is documented for auditing and policy reinforcement. Post-violation, relevant policies are reviewed and updated to prevent future occurrences.

Adhering to these policies is vital for upholding NatureGarden's commitment to professional conduct, security, and the safety of all stakeholders.

### **Regularly updating NatureGarden's Security and Compliance Policy Suite is crucial for several reasons:**

The practice of regularly updating and introducing new regulations and standards, as demonstrated in NatureGarden's Security and Compliance Policy Suite, is a fundamental aspect of maintaining a robust and effective security posture. This approach is beneficial for several reasons:

**Adaptation to Evolving Threats:** The cybersecurity landscape is dynamic, with new threats and vulnerabilities emerging constantly. Regular updates to policies ensure that defences remain relevant and effective against the latest cyber threats. [25]

**Technological Advancements:** As technology evolves, so do the tools and methods for both attacking and defending digital assets. Updated policies can incorporate new security

technologies and methodologies, ensuring that defences are not only current but also forward-looking. [25]

**Compliance with Legal and Regulatory Changes** [25]: Regulations and standards in data protection and cybersecurity are continually evolving. Regular updates help ensure compliance with the latest legal requirements, reducing the risk of penalties and enhancing trust among stakeholders. [25]

**Risk Management:** Updated policies reflect an understanding of the changing risk landscape. They allow for proactive identification and mitigation of potential vulnerabilities, thereby strengthening overall security. [25]

**Stakeholder Confidence:** Regularly updated policies demonstrate to customers, partners, and employees that the organization is committed to security and data protection. This enhances trust and confidence in the company's ability to safeguard sensitive information. [25]

**Best Practice and Industry Standards Alignment:** Updating policies ensures alignment with industry best practices and global standards. This alignment not only enhances security but also positions the organization favourably in a competitive market. [25]

**Employee Awareness and Training:** Regular updates necessitate ongoing training and awareness programs for employees. This keeps security at the forefront of organizational culture and ensures that employees are knowledgeable about the latest security protocols. [25]

**Business Agility and Resilience:** In an ever-changing business environment, updated policies contribute to organizational agility and resilience. They enable the company to quickly adapt to new threats, technologies, and market conditions. [25]

In conclusion, NatureGarden's practice of regularly revising its Security and Compliance Policy Suite exemplifies a commitment to robust security governance. It is a proactive approach that prepares the organization to effectively handle current and future security challenges, ensuring the protection of its assets, reputation, and stakeholders in the digital age.

## References

- [1] "www.6clicks.com," 6clicks, [Online]. Available: <https://www.6clicks.com/resources/answers/what-are-isms-standards>. [Accessed 24 12 2023].
- [2] "www.md7.com," md7, [Online]. Available: <https://www.md7.com/perspectives/md7-reinforces-securing-clients-data-as-highest-priority/>. [Accessed 24 12 2023].
- [3] "www.cyber.gc.ca," Government of Canada, [Online]. Available: <https://www.cyber.gc.ca/en/guidance/guidance-cloud-security-assessment-and-authorization-itsp50105>. [Accessed 23 12 2023].
- [4] "cloudsecurityalliance.org," cloudsecurityalliance, [Online]. Available: <https://cloudsecurityalliance.org/blog/2020/10/16/what-is-the-cloud-controls-matrix-ccm/>. [Accessed 24 12 2023].

- [5 "cpl.thalesgroup.com," Thales, [Online]. Available: <https://cpl.thalesgroup.com/faq/data-security-cloud/what-cloud-controls-matrix>. [Accessed 24 12 2023].
- [6 S. A. I. Umma Khatuna Jannat Dr.MohanKumar, "Adoption of the cloud control matrix framework for effective measurement at cloud risk,threat,attack and vulnerabilit," *International journal of creative research thoughts*, vol. 10, no. 9/9/2022, 2022.
- [7 "cloudsecurityalliance.org," cloudsecurityalliance, [Online]. Available: <https://cloudsecurityalliance.org/blog/2023/11/22/optimizing-your-security-posture-harnessing-the-cloud-controls-matrix-ccm-for-comprehensive-framework-mapping/>. [Accessed 24 12 2023].
- [8 "www.globalreach.com," globalreach, [Online]. Available: <https://www.globalreach.com/faqs/what-is-gdpr>. [Accessed 23 12 2023].
- [9 "commission.europa.eu," European Commission, [Online]. Available: [https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/what-are-main-aspects-general-data-protection-regulation-gdpr-public-administration-should-be-aware\\_en](https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/what-are-main-aspects-general-data-protection-regulation-gdpr-public-administration-should-be-aware_en). [Accessed 24 12 2023].
- [1 "www.itgovernance.co.uk," itgovernance, [Online]. Available: <https://www.itgovernance.co.uk/gdpr-compliance-checklist#:~:text=GDPR%20compliance%20is%20an%20ongoing,security%20controls%20and%20conducting%20DPIAs..> [Accessed 24 12 2023].
- [1 "www.techtarget.com," techrtarget, [Online]. Available:  
1) [https://www.techtarget.com/whatis/definition/acceptable-use-policy-AUP#:~:text=An%20acceptable%20use%20policy%20\(AUP\)%20is%20a%20document%20stipulating%20constraints,being%20granted%20a%20network%20ID..](https://www.techtarget.com/whatis/definition/acceptable-use-policy-AUP#:~:text=An%20acceptable%20use%20policy%20(AUP)%20is%20a%20document%20stipulating%20constraints,being%20granted%20a%20network%20ID..) [Accessed 28 12 2023].
- [1 "support.microsoft.com," microsoft, [Online]. Available: <https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb>. [Accessed 30 12 2023].
- [1 "www.techtarget.com," techtarget, [Online]. Available:  
3) <https://www.techtarget.com/searchsecurity/definition/two-factor-authentication>. [Accessed 28 12 2023].
- [1 "static.spiceworks.com," techrepublic, [Online]. Available:  
4) <https://static.spiceworks.com/attachments/post/0000/4131/SoftwareInstallationPolicy.pdf>. [Accessed 28 12 2023].
- [1 "www.gov.uk," www.gov.uk/, [Online]. Available:  
5) <https://www.gov.uk/government/consultations/unauthorised-access-to-online-accounts-and-personal-data/call-for-information-unauthorised-access-to-online-accounts-and-personal-data>. [Accessed 28 12 2023].

- [1 "www.cps.gov.uk," www.cps.gov.uk, [Online]. Available: <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance>. [Accessed 28 12 2023].
- [1 "ico.org.uk," ico.org.uk, [Online]. Available: <https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/blogs/data-sharing-when-is-it-unlawful/>. [Accessed 28 12 2023].
- [1 "www.techtarget.com," www.techtarget.com, [Online]. Available: <https://www.techtarget.com/searchitoperations/definition/hardware-security>. [Accessed 28 12 2023].
- [1 "resources.workable.com," resources.workable.com, [Online]. Available: <https://resources.workable.com/internet-usage-policy>. [Accessed 29 12 2023].
- [2 "ico.org.uk," ico.org.uk, [Online]. Available: [https://ico.org.uk/media/for-organisations/documents/1563/ico\\_bring\\_your\\_own\\_device\\_byod\\_guidance.pdf](https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf). [Accessed 29 12 2023].
- [2 "www.upguard.com," www.upguard.com, [Online]. Available: <https://www.upguard.com/blog/information-security-policy>. [Accessed 30 12 2023].
- [2 "ico.org.uk," ico.org.uk, [Online]. Available: <https://ico.org.uk/media/about-the-ico/policies-and-procedures/4021371/social-media-use-policy.pdf>. [Accessed 30 12 2023].
- [2 "www.ncsc.gov.uk," www.ncsc.gov.uk, [Online]. Available: <https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles>. [Accessed 30 12 2023].
- [2 "www.gov.uk," www.gov.uk, [Online]. Available: <https://www.gov.uk/intellectual-property-an-overview>. [Accessed 30 12 2023].
- [2 "cybertechworld.co.in," [Online]. Available: <https://cybertechworld.co.in/adapting-to-enhance-cyber-resiliency/#:~:text=Continuous%20monitoring%20of%20your%20security,that%20may%20indicate%20evolving%20threats..> [Accessed 30 12 2023].