Cybersecurity Business Plan

developed for

SwiftCom Solutions Inc.

On

April 04, 2024

SwiftCom Solutions

Connecting Communities, Enriching Lives

Developed by Meenu Handa

Table of Contents

1. Company Introduction

SwiftCom Solutions Inc. is a Canadian telecommunication company operating primarily in the fields of wireless communications, cable, and Internet, with significant additional telecommunications and mass media assets. With a strong customer base and a reputation for quality service, the company has been steadily growing over the years.

SwiftCom was founded in 2020 by Robert Daichenko with a clear vision to revolutionize the telecommunications landscape. Recognizing the growing need for reliable and high-speed internet, phone, and cable services, Robert Diachenko set out to establish a company that prioritizes customer satisfaction, technological innovation, and community engagement. Over the years, SwiftCom has expanded its operations, serving residential and business customers across a diverse range of markets across Alberta and British Columbia with headquarters in Calgary, Alberta.

SwiftCom's journey has been guided by its vision, mission, and core values.

- **Vision:** To be the leading provider of innovative telecommunications solutions, connecting communities and empowering individuals through reliable and accessible communication services.
- **Mission:** Connecting Communities, Enriching Lives.
  Through cutting-edge technology, exceptional customer service, and a dedication to integrity, SwiftCom strives to exceed expectations and drive positive change in the telecommunications industry to deliver seamless connectivity solutions that enhance the lives of its customers.
- **Core Values:**
  - **Integrity:** Upholding honesty and ethical behaviour in all interactions and decisions.
  - **Transparency:** Openly communicating information and processes, promoting clarity and trust within the organization and with customers.
  - **Accountability:** Taking responsibility for actions, delivering on commitments, and owning the outcomes.

2. Executive Summary

In the pursuit of digital excellence, SwiftCom Solutions acknowledges the paramountcy of formidable security protocols, which are essential in the protection of delicate information and the sustenance of consumer confidence. In light of this necessity, SwiftCom has procured the services of a reputable entity to execute an ISO 27001 gap analysis, thereby initiating an exhaustive evaluation of security control gaps, risk analysis, and risk governance measures.

The ISO security control gap assessment has proven to be pivotal in identifying discrepancies between SwiftCom's extant security protocols and the stringent requirements of ISO standards. This critical analysis has facilitated the strategic identification of vulnerabilities, thereby enabling SwiftCom to systematically prioritize security enhancements. This will bolster its defensive mechanisms and ensure compliance with international norms. The assessment has culminated in recommendations that encompass the formulation of quantifiable goals and enduring targets, which will guide SwiftCom's systematic advancement toward achieving exemplary security benchmarks.

In light of the discerned deficiencies and the dynamic nature of the security domain, SwiftCom is prepared to enhance its information security cadre by enlisting proficient individuals capable of executing security-related duties that correspond with their specified functions and accountabilities. This deliberate augmentation is aimed at guaranteeing the efficacious enactment and administration of SwiftCom's security protocols, consistent with the company's strategic goals.

Concurrently, the risk assessment procedure has enabled SwiftCom to conduct a thorough examination of prospective dangers and weaknesses that pose a risk to its business continuity. Through a structured risk analysis, SwiftCom is prepared to proactively establish preventive measures and countermeasures, effectively reducing the probability and impact of security breaches.

Moreover, the risk management dimension of this endeavor highlights SwiftCom's steadfast dedication to the meticulous oversight of risks, not merely their identification. By adopting a forward-thinking and structured methodology for risk management, SwiftCom aspires to bolster its defenses against cyber threats, thereby curtailing the likelihood of adverse financial, operational, and reputational outcomes.

In synopsis, SwiftCom's proactive commitment to ISO 27001-hole appraisal and resulting security drives highlights its devotion to strengthening its security act, shielding delicate information, and saving client trust in the midst of the steadily advancing computerized scene.

ISO 27001 and ISO 27002

ISO 27001 and ISO 27002 are both standards developed by the International Organization for Standardization (ISO) to address information security management. While they are related, they serve slightly different purposes.

ISO 27001

ISO 27001 stands as the cornerstone of information security management, offering organizations a robust framework to safeguard their sensitive data and ensure the resilience of their information systems. It provides a systematic approach to managing sensitive company information, ensuring its confidentiality, integrity, and availability. It provides a systematic approach to identifying, assessing, and managing information security risks, guiding organizations in the establishment, implementation, and continual improvement of their Information Security Management Systems (ISMS). By adhering to the principles and requirements outlined in ISO 27001, organizations can fortify their defenses against cyber threats, bolster customer confidence, and demonstrate their commitment to protecting sensitive information.

ISO 27002

ISO 27002 complements ISO 27001 by offering comprehensive guidelines and best practices for implementing the controls specified within an ISMS. This invaluable resource equips organizations with a practical roadmap for addressing a wide spectrum of information security challenges, encompassing areas such as access control, cryptography, physical security, and incident response. By leveraging the insights and recommendations outlined in ISO 27002, organizations can enhance the effectiveness of their security measures, navigate complex regulatory landscapes, and foster a culture of resilience and vigilance in the face of evolving cyber threats.

3. Security-Relevant Organizational Issues

SwiftCom Solutions is a medium-sized organization with 150-200 employees working under it. Recently, the organization had a ransomware attack that required the company to pay ransom due to customers' records – name, email, phone numbers, SIN, credit card numbers - being leaked. After the company recovered from this major breach, the primary cause discovered was the phishing email. To address this problem, SwiftCom conducted surveys and questionnaires at the organizational level among employees and it uncovered several pertinent issues.

1. Business and security leaders were working at cross-purposes instead of one goal as LOB executives or managers rarely care about cybersecurity, they think of it as an IT department issue. Poor Communication and a sense of powerlessness among them cause this issue.
2. Less participation of the board in the company's overall security strategy.
3. SwiftCom being a mid-sized organization, the auditors and risk officers are not certified which results in less control over security functions and less coordination among different departments' managers.
4. Lack of Information Security staff, a few primary roles are missing in SwiftCom that need to be hired.
5. Risk assessment needs to be performed as there is a lack of understanding of asset owners, who will be accountable for information security risks in the organizations.

This motivates SwiftCom to make changes in policies or define one strategic goal and make some changes in the organization as well.

4. Cybersecurity Strategy

There is a revised cybersecurity strategy that needs to be established by the organization that will focus on a few parameters discussed below.

4.1. Area of Focus

4.1.1 Hire, Motivate and retain security staff

- SwiftCom must have a strong and motivated CISO (Chief Information Security Officer) in place who will hire, motivate, and retain the right security staff.
- Train from within to retain relatively junior security staff and provide them the opportunity to advance up the ladder to more responsible positions.
- Work with internal and external recruiters with a strong emphasis and track record for being effective at matching the business's cybersecurity needs with the right people.
- Supplement scarce resource pools from additional diverse talent sources.

Top factors for motivating and retaining security resources in the organization are:

- An environment enabling cybersecurity staff to advance their careers.
- Competitive salaries and compensation.
- Business management commitment to strong cybersecurity.
- The ability to work with highly skilled and talented cybersecurity staff. [1]

4.1.2 Clarify security-related business roles

- Efforts are made to increase executive buy-in and disseminate the cybersecurity message across all levels of the organization.
- Formalization of security-related roles within security policies and reinforcement through awareness, training, and communication programs is emphasized.
- Follow-up with business leaders to ensure compliance with security policies is always achieved.
- RACI (responsible, accountable, consulted, informed) matrices serve as useful tools for creating better role definitions and enhancing policy effectiveness.
- Security leaders collaborate with business stakeholders to clarify their own and business leaders' security-related roles. [1]

4.1.3 Earn trust and cooperation from users

- Gaining executive support and formalizing security-related roles and responsibilities in policies is crucial.
- Understanding users' perspectives is essential, as they prioritize their daily tasks over security concerns.
- Non-security business staff members and managers have specific security roles, such as adhering to password and credential management policies.
- Caution is advised in daily interactions with email, web browsing, and the Internet to prevent malware infections.
- Effective communication is key to encouraging users to follow security policies and understand the importance of their actions.
- Positive messaging can motivate users to actively contribute to personal and business security efforts. [1]

4.2. Company-Specific Goals

To fortify cybersecurity defenses and foster a resilient security poster, SwiftCom needs to work on six pivotal strategies for navigating the intricacies of modern cybersecurity challenges.

4.2.1 Develop and Govern a Healthy Business Culture

Security culture is a set of customs and behaviors shared by the community and the correct practice of these customs can minimize the risk for the organization. In this world, the weakest vulnerability is people, and considering this a reason some senior executives do not prioritize cybersecurity, either they do not care or they don't want their name after the breach happens. So, organizations need to develop a healthy business culture using some tactics to protect the organization from cyber threats. Some improvements SwiftCom needs to perform in its security culture:

- Create a new security charter that will provide the organization with a revised definition of security as per the company's culture and values. "At SwiftCom, cybersecurity means protecting our telecommunications infrastructure and customer data with integrity, transparency, and accountability. It's about ensuring reliability and security in everything we do, aligning with our vision of innovation and excellence."
- Security charter must have roles and responsibilities defined to provide clarification on whom to approach and who will be accountable for assets.
- A risk management forum needs to be generated which will provide details of risk owners and will help to review and build risk analyses and treatment plans.
- By reviewing the last 6-12 months of security steering committee meetings, SwiftCom can assess the strengths and weaknesses of its committee members and can propose improvements to them.
- SwiftCom must make a centralized security budget to avoid overlapping multiple security budgets.
- SwiftCom must foster a culture of open communication between stakeholders and security team members.
- Enhance user awareness and training programs such as role-specific training, providing free tools or information to the employees to improve cybersecurity at home as well.

4.2.2 Manage IT Risk in the Language of Business

It is very hard for businesses to understand technical risk analyses due to lacked common terms, definitions, and analysis models. To take accountability for business risk, risk must be presented in a quantified form such as monetary loss because those who do not understand cybersecurity believe businesses should try to avoid or prevent all risks which results in unbalanced business costs. Therefore, for business owners to understand digital risk, it is recommended to adopt ISO 31000 - Risk Management Framework - so that risk can be understood in both technical and business terms.

Recommendations

- Using Open Factor Risk Analysis (FAIR) for any kind of risk to evaluate the probable frequency and magnitude of future loss.
- Preparing business risk context using PESTLE – Political, Economic, Social, Technological, Legal, Environmental – analysis.
- SwiftCom needs to identify strategic risk owners via policy after getting top-level sponsorship from business leaders. Determine risk appetite, and plan risk management processes.
- Create a tiered risk assessment by asking questions – Can the issue be addressed through a Standard Operating Procedure? Is this a risk? Is it above its risk appetite? What is the strategic risk to the business?
- Detailed risk evaluation will be done where data will be collected by using one of the approaches – bottom-up, Business Impact Assessment Information, or systemic risk analysis.
- Risks will be monitored and the risk treatment process will be continued which involves accepting, avoiding, transferring, or mitigating the risk.
- Risks will be explained to business staff, associates, stakeholders, risk owners, board of Directors, and Executives.

4.2.3 Establish a Control Baseline.

To specify a minimum set of security controls for the business IT environment and prioritize which control implements to which business units, region or system called control baseline. For example, some controls might apply to systems with confidential data but not to systems with public data. After implementing those controls, verify controls are operating correctly. ISO 27001

- For SwiftCom, two lines of defense meta-model combination of architecture and governance will be used to verify and confirm controls.
- SwiftCom's control baseline must be aligned with third party through shared responsibility models and should work together by asking these questions for different perspectives such as What controls must the customer operate to secure the use case? What controls (or capabilities) should the third party provide to the customer? How should the customer evaluate the general security posture of the third party to know whether to trust it? What controls that the third party is solely responsible for should customers most rigorously evaluate?
- Tune controls using variables such as risk and compliance, cost and maintenance, customer needs, and user experience that style with business needs and risks after engaging IT stakeholders.
- Scaling and aligning the control baseline keeping maturity requirements in mind such as governance, and access management.

4.2.4 Simplify and Rationalize IT and Security

To secure something, one must know how to manage it. In a chaotic IT environment, it is difficult to implement a control baseline. Effective security management relies on managing IT infrastructure, but implementing controls in complex environments is challenging. While security leaders don't own IT strategy, they advocate for simplicity. Outdated IT setups underscore the need for cloud adoption and modern practices. IT must streamline infrastructure and shift towards a "broker" model for cloud management. Collaboration between IT, innovation, and cybersecurity is key for crafting strategies prioritizing agility and risk reduction. Security leaders promote best practices like tiered risk assessments and DevSecOps, aiding in effective strategy development. Their cross-functional role fosters alignment with organizational goals.

- Developing strategy that will leverage the inherently cross-functional roles security to help improve the IT or digital architecture and strategy by reducing macro-complexity and simplifying micro-complexity, working on predefined IT strategy and coordinating function between IT, LOBs, and corporate administration groups.
- IT and security organizations develop a service catalog of shared capabilities to reduce the risk of the shadow of IT.
- Including security services in the IT service catalog such as contracts, cost models, and service level agreements.
- Leverage the cross-functional roles security is naturally asked to perform – as policy establisher, access gatekeeper, and security service enabler – to help improve the IT architecture and strategy.
- Coordinate the asset inventory control and asset risk profiling implementation, timing, and data models with those of IT- or EA-led application consolidation and rationalization efforts.
- Support forward-thinking IT leaders seeking to establish IT-as-broker in the cloud environment and/or finance projects working to put technical debt on the balance sheet.
- Cross-fertilize security staff or expertise into development and/or operations organizations to establish risk-informed DevSecOps and Disciplined Agile practices.

4.2.5 Control Access with Minimum Drag on Business

In information security, implementing access control and data governance, including IAM systems, is vital for preventing breaches and ensuring data privacy compliance. IAM's technical complexity and human-centric nature require collaboration across business, IT, and development domains. While access control safeguards assets, digital identities enable business operations, amplifying privacy and regulatory risks. This module offers insights into access control, IAM development, balancing access control and responsibility, modernizing IAM for digital business, monitoring identity events, and implementing IAM and data governance strategies. It is recommended that:

- Control baseline activities should be operated in IT systems as well as critical assets with continuous discussion with internal development team to implement controls in case of any changes.
- Work with stakeholders such as the business's Privacy Office, executives, enterprise architecture (EA), and digital initiative leaders to understand how the business culture should drive design principles for identity governance, data governance, access control, and accountability. Adopting a "trust but verify" approach allows for discretion while promoting accountability, so there should be a balance between risk and productivity. Accountability-based controls empower users and managers, supported by positive reinforcement and enforcement measures to ensure compliance.
- IAM teams must often enhance identity interoperability standards support in the business applications and infrastructure by managing digital relationships and taking a proactive approach to privacy.
- Deploy IGA systems to manage role-based access to critical processes and PAM systems to protect critical assets.
- Establish an IAM working group enabling the IAM team, developers, and other IT or security groups to exchange knowledge and work on processes, role models, or technical standards.
- IAM teams should work with business developers to share new and existing applications' privacy requirements and business models.
- Engage HR, compliance, and appropriate IT or development functions in creating roles for provisioning birthright accounts, managing centralized IT services, and securing applications with compliance-mandated roles.

4.2.6 Institute Resilient Detection and Response

Cyber-resilience empowers businesses to withstand and mitigate information risks by identifying critical assets, top-risk scenarios, and contingency plans. Aligning technical security capabilities with IT operations and other functions enables early detection of suspicious events and swift response to incidents like breaches or outages. Incident response, closely tied to monitoring and detection, demands dedicated management coordinating with various departments. Structured response plans for common incidents ensure coordinated action across functions. Recovery from serious incidents requires business impact assessments and continuity plans to restore critical assets, necessitating coordination between business continuity and incident response teams.

- Identify critical assets through a Business Impact Analysis and create a Business Continuity and disaster recovery plan.
- Analyse top risk scenarios through enterprise risk assessment and document risk appetites.
- Prepare contingency plans for coping with outages, breaches, and other incidents from cybersecurity maturity assessment, incident response planning, and cyber-insurance coverage acquisition.
- Plan for unexpected incidents, and detect cybersecurity events by Monitoring Event Logs, Alerts, and Reports and standardizing basic logging, log collection, and log review across IT environments.
- Respond to incidents in the following steps:

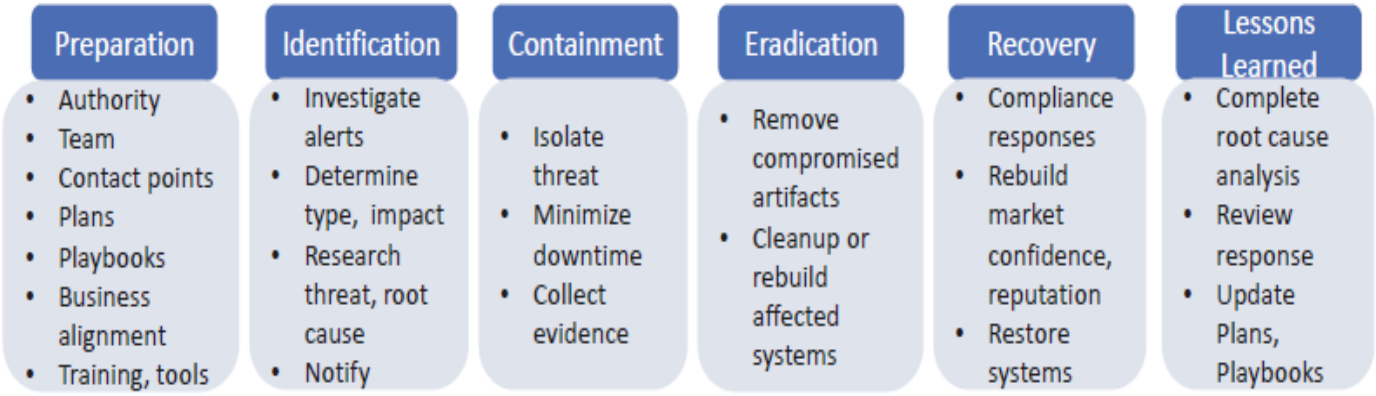


Figure 1 *- Steps for responding to incidents*

- Planning separate but overlapping processes for responding to cyberattacks and operational outages.
- Ensuring that senior business stakeholders support the business continuity program and that the key IT team members who work "hands-on" with mission-critical services are engaged.

4.3 Goal Timelines and Success Metrics

Establishing and measuring success metrics is an important skill for business leaders to develop so that they can monitor and evaluate their team's performance. It is a quantifiable measurement that business leaders need to track to see if their strategies are working effectively. To implement the improvement objectives in SwiftCom, goal timelines are set for 30 days, 60 days, and 90 days' time with the success metrics.

- The Security Charter will be revisited and the definition of security will be redefined as per SwifCom's mission, values and for that stakeholder meeting will be scheduled 2 times in 30 days to plan and finalize.
- New security roles will be discussed which are planned to be hired in 90 days.
- Meeting with stakeholders to define who are the asset owners or risk owners.
- Control baseline will be set as per the top risks and countermeasures/safeguards against those risks.

5. Applicable Legal and Regulatory Requirements

As SwiftCom Solutions navigates the dynamic landscape of cybersecurity, it must intricately weave through the intricate tapestry of legal and regulatory frameworks governing the telecommunications industry. In an era where data breaches and privacy issues frequently make headlines, SwiftCom's cybersecurity strategy must not only protect against emerging threats but also adhere to a multitude of strict regulations. By meticulously aligning its security protocols with these legal requirements, SwiftCom not only strengthens its defenses but also fosters trust among its clients, solidifying its reputation as a responsible guardian of sensitive information.

In the domain of telecommunications and data privacy in Canada, three crucial regulatory bodies take center stage: the Canadian Radio-television and Telecommunications Commission (CRTC), the Personal Information Protection Act (PIPA), and the Control Objectives for Information and Related Technologies (COBIT). The CRTC acts as the authoritative body overseeing broadcasting and telecommunications regulations, ensuring compliance with laws designed to foster fair competition and safeguard consumer interests. PIPA outlines guidelines for collecting, using, and disclosing personal information by private organizations within Alberta and British Columbia. Collectively, these regulations serve as the foundation for data protection and privacy governance within organizations. COBIT offers a comprehensive set of principles, practices, and guidelines that help SwiftCom establish robust governance frameworks, define clear control objectives, and improve the overall performance and reliability of its IT systems. By adopting COBIT, SwiftCom

can enhance its IT governance practices, strengthen cybersecurity measures, and drive greater business value through IT investments.

Personal Information Protection Act (PIPA)

PIPA is an act about privacy in the private sector. It helps protect the personal information of the public (your customers) and your employees. It creates common-sense rules about collecting, using and disclosing (showing, telling or giving some other organization) personal information. The Act balances:

- an individual's right to have his or her personal information protected, and
- an organization's need to collect, use or disclose personal information for purposes that are reasonable, that is, for legitimate business purposes.

The Act also gives individuals the right to ask an organization to show them the personal information it has about them and to ask for the information to be corrected if they think the information is incomplete or inaccurate. PIPA applies to all organizations and all personal information held by organizations unless the Act says that it does not apply. IPPA's guidelines for the organizations:

- Be accountable.
- Get consent.
- Follow the rules for collecting, using, and disclosing information.
- Follow special rules for employee information, and business transactions.
- Follow the rules for giving access to, and correcting personal information. [2]

Canadian Radio-television and Telecommunications Commission (CRTC)

The Canadian Radio-television and Telecommunications Commission (CRTC) is an independent public authority that creates and enforces rules that govern Canada's radio, television, and telecom sectors. Those rules affect what you do and don't see on TV, hear on the radio, and the price and accessibility of your phone and internet services. The CRTC is run by commissioners, including a chairperson, who are appointed by the Cabinet — specifically the Heritage Minister. The decisions the CRTC makes directly impact the price of your Internet and phone bills and your ability to access high-quality and affordable services. They have the power to affect the Canadian telecom market and how different companies interact in the industry.[3]

Control Objectives for Information and Related Technologies (COBIT)

COBIT is an IT governance framework for businesses wanting to implement, monitor, and improve IT management best practices. The COBIT framework was created by ISACA to bridge the crucial gap between technical issues, business risks, and control requirements. COBIT can be implemented in any organization from any industry to ensure the quality, control, and reliability of information systems. The goal of the COBIT framework is to provide a common language for IT professionals, business executives, and compliance auditors to communicate with each other about IT controls, goals, objectives, and outcomes. Without a common language, an enterprise under audit runs the risk of having to educate individual auditors about when, where, how, and why specific IT controls were created. COBIT incorporates more than just technical standards for IT managers. The framework supports business requirements through the combined application of IT, related sources, and processes. Two main parameters provided are:

- **Control:** Includes IT management procedures, practices, policies, and structures designed to provide an acceptable level of assurance that business goals will be met.
- **IT control objective:** Defines the level of acceptable results to be attained by implementing control procedures concerning a particular IT operation.

COBIT is based on five key principles for IT enterprise governance:

- Principle 1: Meeting Stakeholder Needs
- Principle 2: Covering the Enterprise End-to-End
- Principle 3: Applying a Single Integrated Framework
- Principle 4: Enabling a Holistic Approach
- Principle 5: Separating Governance from Management [4]

6. Roles and Responsibilities

To ensure the effectiveness of our defense strategies against evolving threats, it is paramount to delineate clear roles and corresponding responsibilities in the organization. Each individual in the organization plays a critical role in safeguarding SwiftCom's digital assets, protecting sensitive customer data, and fortifying our resilience against cyberattacks. In this section, we outline some specific roles and responsibilities that the organization's cybersecurity team will take.

6.1 Board of Directors

The Board of Directors acts as the governing body and plays a vital role in offering strategic direction, supervision, and accountability. Responsibilities of the Board of Directors include: [5]

1. The Board must acknowledge that cybersecurity is a significant risk affecting the entire organization and it is not just an IT concern. This involves grasping its potential effects on operations, finances, and reputation.
2. Directors need to understand the legal implications of cyber risks within the company's context, ensuring adherence to applicable laws and regulations to minimize legal vulnerability.
3. The Board will communicate with cybersecurity experts and allocate sufficient meeting time to discuss effective strategies for managing cyber risks which helps safeguard the organization against potential threats and ensures a robust defense against cyber risks.
4. Directors should communicate their expectations to management regarding creating an organization-wide risk management framework. This involves allocating adequate staffing and budget resources to effectively address cybersecurity.
5. During management discussions, it's essential to identify risks that should be avoided, accepted, or mitigated using diverse strategies. This alignment ensures consistency with the company's risk tolerance and strategic goals.

Although the Board of Directors should not manage details of security programs, it should have a good understanding of what information risks mean to the business and a committee structure through which it can set direction for risk management. [1]

6.2 Chief Executive Officer (CEO)

As CEO, ultimate accountability for cybersecurity falls on ensuring proper management, addressing risks, and fostering transparency and collaboration. Responsibilities include:

1. As the top business executive, the CEO serves as a commander and holds ultimate accountability and decision-making authority. While they may entrust security leaders with specific duties, they ultimately bear responsibility to the Board and the public for any significant shortcomings/ security failures.
2. CEOs must also address cybersecurity-related objectives with their direct reports and ensure the right people are in place and managing cybersecurity. [1]
3. CEOs must identify and address systemic risks within the organization such as decisions that compromise security readiness. For example, refusing to shut down a server for proper patching. [6]
4. Involves fostering a culture of openness and accountability within the organization, where boards and executives are encouraged to acknowledge the imperfections in security measures. This includes facilitating

discussions about existing gaps and opportunities for improvement, ensuring that both IT and non-IT executives are informed about the realities and limitations of cybersecurity, and collaborating to address challenges effectively. [6]

6.3 Chief Counsel (Legal)

Chief Counsel approves or manages security-related content contracts with employees, third parties such as vendors and contractors, and the participants in mergers, acquisitions, and joint ventures. It has input and approval on the following security-related functions:

1. Audit, compliance, and HR-related security issues.
2. Breach investigations, responses, and notifications.
3. Security policies.
4. Estimating liability risk. [1]

6.4 Chief Information Security Officer (CISO)

As the guardian of digital assets and defender against cyber threats, the Chief Information Security Officer (CISO) holds a crucial position in the organization. Tasked with creating and implementing strong security protocols, the CISO safeguards the integrity, confidentiality, and accessibility of the company's information assets. Responsibilities include:

1. CISO will be responsible for running cybersecurity programs such as developing and implementing the organization's information security strategy, and establishing/ enforcing security policies and procedures.
2. CISO will represent cybersecurity functions internally and externally such as being the primary liaison with regulatory bodies, auditors, and external security vendors. Also, collaborating with other executives and departments to align security initiatives with business objectives.
3. Lead incident response and recovery efforts in the event of a security breach.
4. Monitoring and analyzing security metrics and reports to ensure compliance and effectiveness.
5. Providing cybersecurity awareness training to employees.
6. Identifying and assessing security risks and vulnerabilities.

6.5 Chief Information Officer (CIO)

CIO plays a crucial role in ensuring the company's continued growth and success in a rapidly evolving digital landscape. The CIO's position is one level down from CEO and reports to CXO below the CEO. Responsibilities include:

1. Managing the IT budget and resources effectively.
2. Ensuring alignment between technology investments and business goals.
3. Providing leadership and guidance to IT staff, fostering a culture of innovation and excellence.
4. Setting the organization's overall technology strategy and vision.

6.6 Audit and Compliance Officer

Audit and Compliance officer manages the communication between business executives, IT, and external auditors. The audit is an important "check and balance" on the other IT security functions. The officer will ensure that personal information is protected and that other compliance requirements are met. Responsibilities include:

1. Developing and implementing audit and compliance programs with recommended corrective plans for non-compliance areas.
2. Conducting internal and external audits to assess the effectiveness of internal controls and compliance with policies and regulations.
3. Monitoring changes in laws and regulations and updating policies and procedures accordingly.

4. Reporting audit findings and compliance status to senior management and the board of directors.
5. Investigating allegations of non-compliance or unethical behavior.

6.7 Chief Risk Officer (CRO)

A CRO will oversee Enterprise Risk Management (ERM) in the organization. Responsibilities include but not limited to:

1. CRO will develop and implement risk management strategies and policies to identify or assess risks across the organization.
2. Establish risk tolerance levels and limits and report to senior management and the board of directors.
3. Develop and maintain risk management frameworks and processes ensuring compliance with regulatory requirements.

6.8 Incident and Access Management (IAM) Manager

IAM Manager plays a vital role and is responsible for ensuring the secure and efficient management of user identities, permissions, and access across the organization's systems and applications as well as IAM strategies. Responsibilities include:

1. Developing IAM strategies, policies, and procedures and providing training to employees.
2. Conduct regular audits to identify and remediate security risks and violations.
3. Collaborate with IT and security teams to integrate IAM solutions into the organization's infrastructure and applications.
4. Implementing and maintaining IAM technologies, such as multi-factor authentication.
5. Ensuring compliance with security best practices related to identity and access management.

6.9 IT Operations

IT Operations serve as the backbone of technological functionality and efficiency as well as ensure seamless functionality and optimal performance across the organization's IT landscape. Responsibilities include:

1. Managing and maintaining servers, databases, and other IT infrastructure to ensure optimal performance, reliability, and security.
2. Configuring, monitoring, and troubleshooting network devices, such as routers, switches, and firewalls, to ensure connectivity and data integrity.
3. Implementing and maintaining backup solutions to protect data integrity and facilitate disaster recovery efforts in case of data loss or system failure.
4. Applying software patches and updates to servers, workstations, and other devices to address security vulnerabilities and ensure system stability.

6.10 Security Incident Response/ Security Ops Manager

Security Incident Response encompasses identifying, probing, and mitigating security incidents. It involves coordinating responses, communicating with stakeholders, implementing remedial actions, and continuously enhancing cybersecurity resilience. Responsibilities include:

1. Detecting and identifying security incidents and breaches.
2. Investigate security incidents to determine the cause and extent of the breach.
3. Containing and mitigating the impact of security incidents to minimize damage and disruption.
4. Coordinating response efforts across various teams, including IT, legal, and communication teams.

6.11 Human Resources

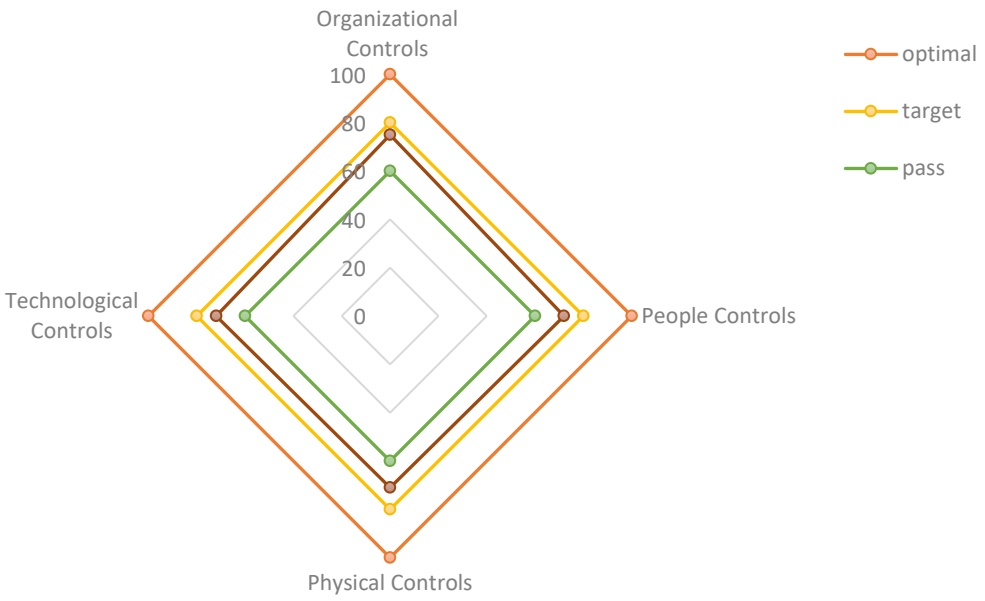
HR performs background checks on new hires and has a role in onboarding all new staff as well as hiring staff for the security team. It also has oversight of or provides input and approval for the following security-related functions:

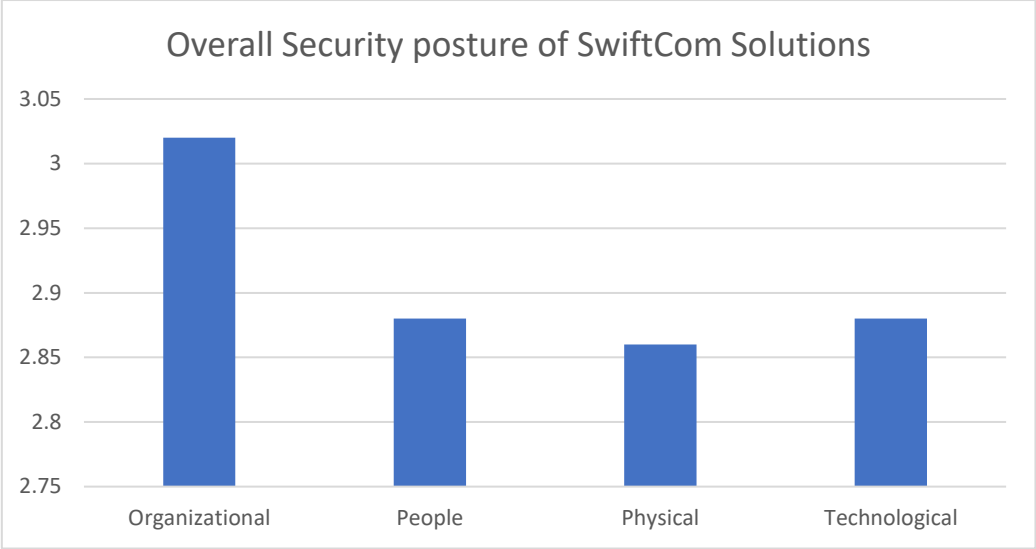
1. Personnel-related security policy (e.g., for acceptable use policy or bring your own device (BYOD) policy).
2. Security-related roles and responsibilities (e.g., do they comply with personnel policies, union rules).
3. Disciplinary actions for security policy violations.
4. Incentive programs to promote better risk management or security behavior.
5. User awareness training content. [1]

7. Results of Security Control Gap Assessment ISO 27001:2022

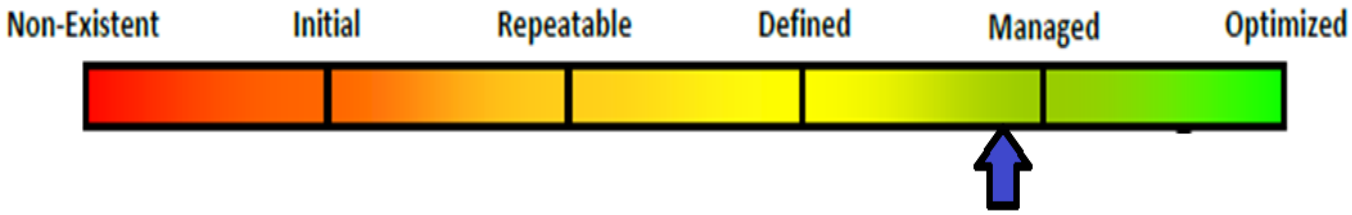
After performing ISO 27001:2022 gap assessment on SwiftCom Solutions, there are many findings that the company needs to improve. Many controls have been suggested to implement and there are a few controls that re implemented but not practiced regularly. This section will cover the gaps and some recommendations on how to implement those.

7.1 Summary of Results Overview

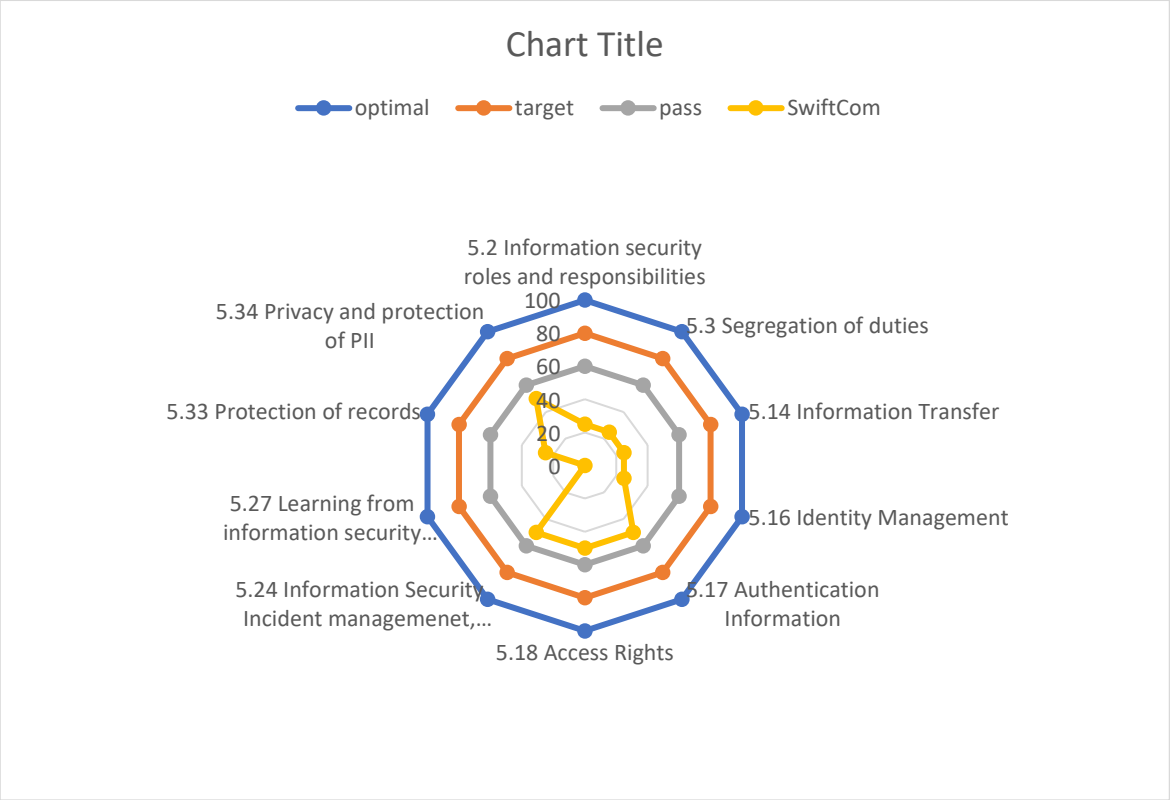




7.2 Organizational Security Controls



Overall Current Score: 3.02



Control 5.2: Information Security roles and responsibilities

Current Score: 1

Current Maturity Level: Performed Informally

Objective: To establish a clear, authorized, and comprehended framework for implementing, operating, and overseeing information security across the organization.
Observation: No documentation was created for clearly outlining roles and responsibilities.

Recommendation: Clearly outline the roles and responsibilities related to information security within policies and procedures, ensuring they are straightforward and readily accessible for all pertinent staff members.

Control 5.3: Segregation of duties

Current Score: 1

Current Maturity Level: Performed Informally

Objective: This control aims to separate conflicting duties.

Observation: Which duties require segregation was not documented.

Recommendation: Establish role-based access controls (RBAC) to maintain duty separation, guaranteeing that personnel have access solely to the systems and information required for their designated roles and duties.

Control 5.14: Information Transfer

Current Score: 1

Current Maturity Level: Performed Informally

Objective: This control mandates organisations to install the necessary procedures to maintain data security when shared internally or sent to external parties.

Observation: Organization needs to place guidelines for verbal and electronic transfer of data.

Recommendation:

- Rooms used for confidential conversations should be fitted with necessary soundproofing.
- Confidential matters must not be discussed in public areas.
- Implementing strict authentication methods and ensuring communications are sent to the appropriate recipients by avoiding the risk of sending to the incorrect email address, address, or phone number.

Control 5.16: Identity Management

Current Score: 1

Current Maturity Level: Performed Informally

Objective: To establish a framework for approving, registering, and administering human and non-human identities on any network.

Observation: Organisation cannot identify who (**users, groups of users**) or what (**applications, systems, and devices**) is accessing data or IT assets at any given moment, and how those identities are granted access rights.

Recommendation:

- Identity management must be documented. If an identity is assigned to an employee, that person is the only one who can authenticate with that identity and it should be noted.
- A 'one entity, one identity' rule should be followed to avoid duplicate identities. Approach of shared identity should be used only when an explicit set of operational requirements is needed.

Control 5.17: Authentication Information

Current Score: 2

Current Maturity Level: Planned

Objective: It states that user credentials such as passwords, security questions must be secure from unauthorized access.

Observation: Employees are either using default or easy guessable common passwords.

Recommendation:

- Upon enrolment of new employee, default passwords must be changed to strong secure passwords that should be in compliance with industry standards such as passwords must not be based on personal information.
- SwiftCom should have their employees accept the responsibility for creating and using passwords in their employment contracts.

Control 5.18: Access Rights

Current Score: 2

Current Maturity Level: Planned

Objective: An organisation can implement procedures and controls to assign, modify, and revoke access rights to information systems as well as physically consistent with its access control policy.

Observation: Information available physically anyone can access that if have access to storage room.

Recommendation:

- SwiftCom should consider the separation of duties.
- A person's access rights should be immediately revoked when they no longer require access to information assets, especially if they have departed the organisation.
- Log and maintain changes to a user's physical and logical access rights are mandatory.

Control 5.24: Information Security incident management, planning and preparation

Current Score: 2

Current Maturity Level: Planned

Objective: To ensure a consistent and practical approach to managing information security incidents, events, and weaknesses.

Observation: When the organization had ransomware attack, there were no logs and planning to handle such events.

Recommendation:

- Develop a documentation for reporting similar security events with single point of contact.
- Incidents or events related to Information security should be managed using five steps Monitoring, detection, classification, analysis, reporting either manually or automation process.

Control 5.27: Learning from Information Security incidents

Current Score: 0

Current Maturity Level: Not Performed

Objective: To make better decisions in the future, it is imperative to learn from information security events or incidents.

Observation: Since there were no logs of previous security events, employees were never aware and given training to handle situations in future.

Recommendation: In incident management framework, projected scenarios and associated procedures must be mention to enhance awareness by discussing how to respond, avoiding and resolving past incidents.

Control 5.33: Protection of Records

Current Score: 1

Current Maturity Level: Performed Informally

Objective: All records must be protected from loss, damage or destruction.

Observation: There was no secure practice to protect records from any loss, damage or destruction.

Recommendation:

- Draft and publish guidelines addressing four main functions record disposal, preventing manipulation, record storage, record handling chain of custody.
- Destroy records in a secure, suitable way as soon as the retention period is complete.
- Categorize records like personal, legal, accounting, business record.

Control 5.34: Privacy and Protection of PII

Current Score: 2

Current Maturity Level: Planned

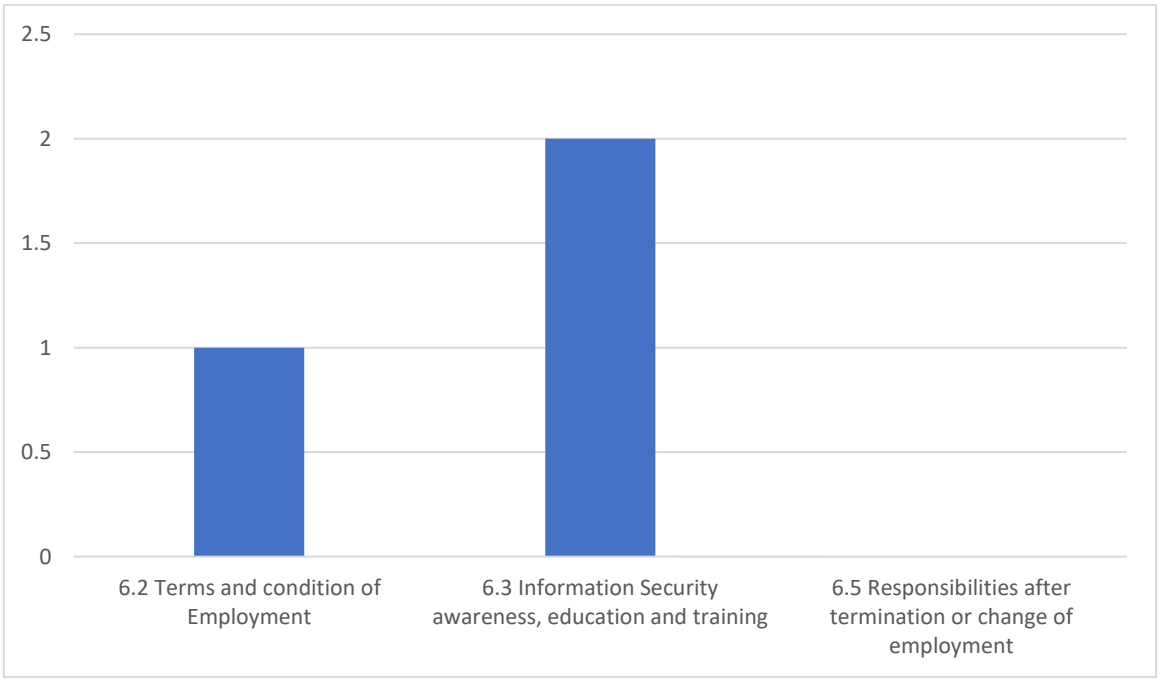
Objective: This control outlines the protection of Personally Identifiable Information (PII) in three distinct areas: privacy, protection, preservation.

Observation: Protection of PII is in the control of organization, policy was last revised in year 2021.

Recommendation: Policy for protection, preservation of PII needs to be updated with some compliance standards and ensuring that all staff members are aware and adhere to it.

7.3 People Security Controls

Overall Current Score: 2.88



Control 6.2: Terms and condition of Employment

Current Score: 1

Current Maturity Level: Performed Informally

Objective: A contractual agreement to inform new employees of their and the company's responsibility for information security.

Observation: In the agreement, employees are not aware of their responsibilities toward protecting company's assets.

Recommendation: The policy needs to be updated to ensure individuals who are given access to confidential information should sign a nondisclosure agreement and their legal rights. If any individual disregards organizational information security requirements, actions need to be taken and explained what they are.

Control 6.3: Information Security awareness, education and training

Current Score: 2

Current Maturity Level: Planned

Objective: It involves informing employees of the significance of information security and inspiring them to enhance their computer security practices.

Observation: Trainings have been conducted but not in regular basis.

Recommendation: With the advancements in cyber-attacks, employees should be educated every month regarding new attacks happening in various organizations to introduce awareness and best practices to perform their job duties without compromising information security and focusing on role-specific training.

Control 6.5: Responsibilities after termination or change of employment

Current Score: 0

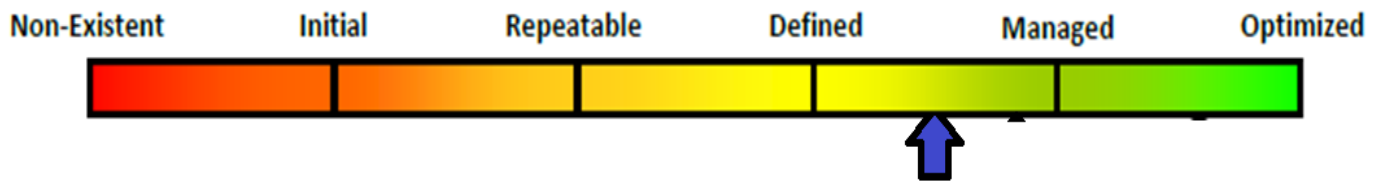
Current Maturity Level: Not Performed

Objective: It is a safeguard against the possibility of employees taking advantage of their access to confidential information and processes for personal gain or malicious intent, especially following their departure from the organization or job.

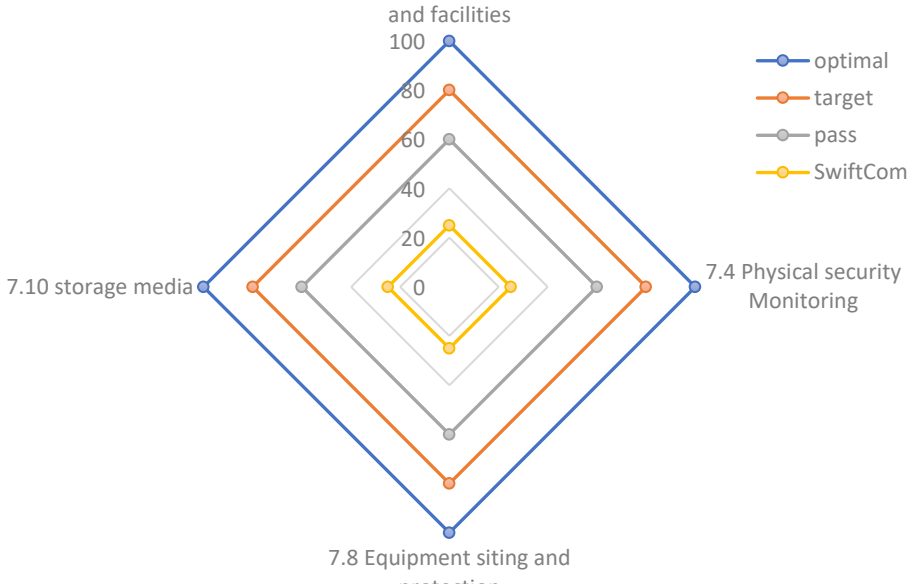
Observation: No security control in place.

Recommendation: Upon termination, it needs to make sure that all access credentials are deleted and replaced. Also, it is essential to communicate the necessary information security and legal requirements, as well as any applicable confidentiality agreements that may run for a specified period following the end of the employee or contractor's engagement.

7.4 Physical Security Controls



Overall Current Score: 2.86



Control 7.3: Securing offices, rooms and facilities

Current Score: 1

Current Maturity Level: Performed Informally

Objective: It outlines the requirement for constructing and executing physical security for offices, chambers and venues.

Observation: Only main door is locked but files can be accessible from the room to those who are not authorized.

Recommendation:

- Secure all doors, windows and cupboards.
- CCTV must be installed for monitoring activity on the grounds or in particular regions of a structure.
- Installing intruder alarms that can sense motion, heat or sound and trigger these alarms.

Control 7.4: Physical security monitoring

Current Score: 1

Current Maturity Level: Performed Informally

Objective: To ensure no access is given to unauthorized person to the restricted area.

Observation: No surveillance tools in place to protect information assets in SwiftCom stores.

Recommendation:

- Security cameras need to install to keep a record of all entries and exits on the premises.
- To prevent any vulnerabilities from being exploited, install alarm system to protect all sensitive areas.

Control 7.8: Equipment siting and protection

Current Score: 1

Current Maturity Level: Performed Informally

Objective: To eliminate or mitigate risks associated with equipment containing information assets such as power outage or damage.

Observation: Equipment containing sensitive information are not placed in secure area.

Recommendation:

- Computers, monitors, and printers must be configured and positioned in such a way so that unauthorised individuals cannot view the information on screens.
- IT equipment must be segregated from equipment not owned or controlled by the SwiftCom to prevent it from unauthorized damage.

Control 7.10: Storage Media

Current Score: 1

Current Maturity Level: Performed Informally

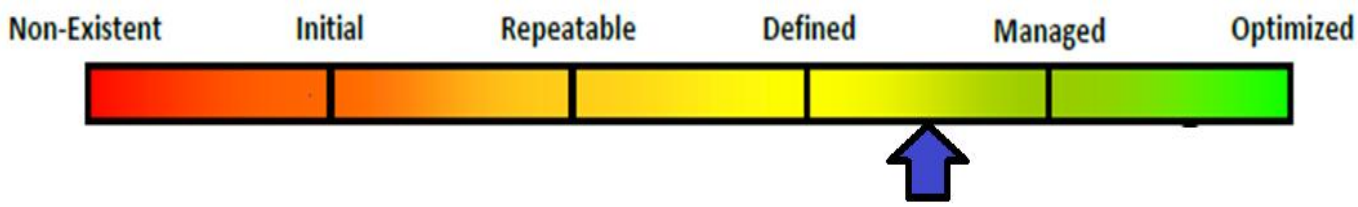
Objective: For organizations to eradicate risks associated with unauthorised access, and transmission of confidential data held on physical and digital storage media such as paper, USBs.

Observation: Policy need to be revise.

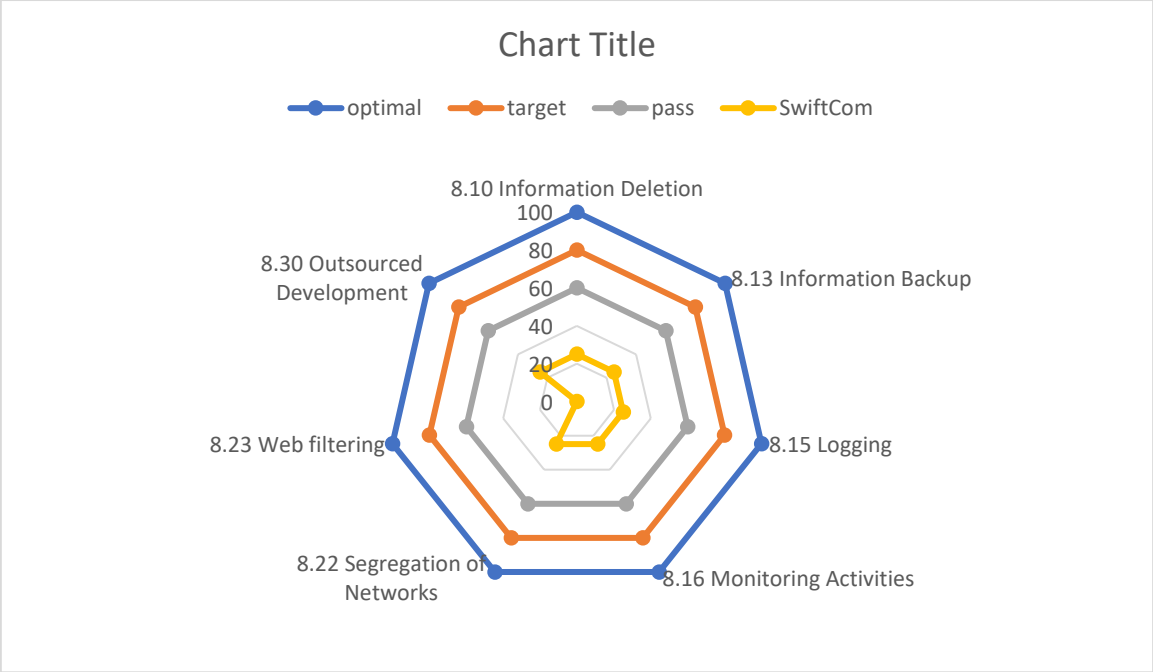
Recommendation:

- Cryptographic methods should be employed to safeguard the media from unauthorised access.
- To prevent deterioration and data loss from digital storage media, the information should be moved to a fresh storage media device before the risk arises.
- When choosing a third-party service for the collection and disposal of storage media, organizations must perform thorough evaluations to ensure the vendor is qualified and possesses the necessary safeguards.

7.5 Technological Security Controls



Overall Current Score: 2.88



Control 8.10: Information Deletion

Current Score: 1

Current Maturity Level: Performed Informally

Objective: An obligation for organization to erase data stored on internal servers, hard drives, arrays and USB drives once it is no longer needed.

Observation: No documentation found that deletion has been performed for unwanted data.

Recommendation: SwiftCom need to specify its needs when using a third-party vendor, including deletion methods and time-frames, and should guarantee that deletion activities are included in a binding contract.

Control 8.13: Information backup

Current Score: 1

Current Maturity Level: Performed Informally

Objective: It outlines how organization's staff involved in maintaining an organisation's network should handle daily backup operations.

Observation: Backups are not maintained properly.

Recommendation:

- Maintain backups in an appropriate location that is environmentally protected, physically separate from the source data, and securely accessible for maintenance.
- Identify all relevant critical systems and services and outline clear and concise restoration procedures.
- Data that has been backed up should be encrypted according to its risk level.
- Make sure maintenance staff are notified of the status of backup jobs so remedial action can be taken if they fail wholly or partially.

Control 8.15: Logging

Current Score: 1

Current Maturity Level: Performed Informally

Objective: It provides an overview of Information and Communication Technology activities and personnel actions.

Observation: Logs are not properly maintained or updated.

Recommendation:

- Log all the attempts to access secure, business-critical resources, such as domain servers, web portals, and file-sharing platforms.
- Gather data usage records from service vendors or internal systems to recognise any malicious behaviour.
- For each event log, it must contain user ID associated with the person, system activity, date and time of event occurred, location and device on which event occurred, network addresses, protocols and IP information.

Control 8.16: Monitoring Activities

Current Score: 1

Current Maturity Level: Performed Informally

Objective: To continuously monitor network for successful security operations.

Observation: Networks are not being monitored properly and no appropriate actions taken to evaluate potential information security incidents.

Recommendation: Actions need to perform to track regular network monitoring in SwiftCom

- Monitor any changes in risk level and modify monitoring activities accordingly.
- React to suspicious data, usage patterns, and user behavior, as well as one-off activities.
- React to intrusion detection, e.g. DDoS attacks, or malicious system behavior such as keylogging.
- Track traffic to and from applications, both inbound and outbound.

Control 8.22: Segregation of Networks

Current Score: 1

Current Maturity Level: Performed Informally

Objective: It will allow to divide IT networks into sub-networks dependent on the degree of sensitivity and importance, and to limit the transmission of information between those different sub-networks.

Observation: SwiftCom has not segregated its network into sub-domains.

Recommendation:

- SwiftCom must consider sensitivity and importance of each network domain and depending on that it should name its sub domain as public domains, server domains.
- For delicate networks, SwiftCom can take all wireless access attempts as external connections and forbid access to internal networks until the gateway control gives approval.
- Personnel should only use their own devices in line with the organization's policy; the network access provided to personnel and guests should be kept separate.

Control 8.23: Web filtering

Current Score: 0

Current Maturity Level: Not Performed

Objective: It eliminates security risks such as malware infection from accessing external websites with malicious content.

Observation: Security control needs to update.

Recommendation: Block websites

- With the capability of uploading information. Obtaining access should be subject to authorisation and only be granted in cases where business reasons are valid.
- That is known or suspected to contain malicious material.
- That distribute materials and content that are illegal.
- Training must be conducted to ensure employees know their own rules and how to report security concerns.
- Training must cover the exception process for accessing restricted websites for legitimate business reasons.
- Training must also cover browser advisory messages that warn users a website isn't secure but allow them to continue. These warnings must be addressed by staff.
- Techniques used for web filtering are: Heuristics, Signatures, List of prohibited and acceptable websites, Domain configuration.

Control 8.30: Outsourced Development

Current Score: 1

Current Maturity Level: Performed Informally

Objective: It will help organisations ensure that the established information security requirements are adhered to when outsourcing system and software development to third parties.

Observation: SwiftCom is not continuously monitoring and verifying that outsourced development work meets the information security requirements set out by the organisation.

Recommendation:

- Implementing a threat model that third parties can adopt.
- Developing and entering into licensing agreements that cover code ownership and intellectual property rights.
- Maintaining evidence that adequate testing has been conducted to address identified vulnerabilities.
- As part of the agreement with the supplier, the organisation should be allowed to audit the development process and controls.
- Security requirements for the development environment should be established and implemented.

8. Results of Risk Assessment

8.1 Classification Scheme

To perform risk assessment for SwiftCom Solutions, there are several steps need to perform:

- Asset Inventory: Identify asset, asset owner, classifying the assets based on criticality of information, and specifying the location of asset.
- Security Impact Analysis: Security impact rating is based on the CIA, regulatory, reputational, Financial basis.

- Threat Exposure rating: Identify threat and assessing how likely will happen.

8.2 Sample Asset Inventory

Asset: Asset is anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards).

Classification: Information assets are assigned a sensitivity level based on the appropriate audience for the information. Information can be classification into types

- Restricted: Highly valuable and highly sensitive to business and the level of protection is dictated externally by legal and/or contractual requirements. It must be limited to only authorized employees, contractors and business partners with specific business needs. It can cause significant damage to company's competitive position, reputation, and contracts.
- Confidential: Highly valuable, sensitive business information and the level of protection is dictated internally by the Company. It can cause moderate damage to the company's reputation, and position and expose the geographic location of individuals.
- Internal use: Information owned and generated by the organization may be shared with authorized employees but not to be released to the general public. It can cause minimal or no damage to the company's reputation.
- Public: Information that has been approved for release to the general public and is freely shareable both internally and externally. It would not cause any damage to the company's reputation.

Classification	Information security classification Description	
Restricted	Definition	Restricted information is highly valuable, highly sensitive business information and the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors, and business partners with a specific business need.
	Potential Impact of Loss	· **SIGNIFICANT DAMAGE would occur if Restricted information were to become available to unauthorized parties either internal or external to your Company.** · **Impact could include negatively affecting your Company's competitive position, violating regulatory requirements, damaging the your Company's reputation, violating contractual requirements, and posing an identity theft risk.**
Confidential	Definition	Confidential information is highly valuable, sensitive business information and the level of protection is dictated internally by your Company
	Potential Impact of Loss	· **MODERATE DAMAGE would occur if Confidential information were to become available to unauthorized parties either internal or external to your Company.** · **Impact could include negatively affecting your Company's competitive position, damaging the your Company's reputation, violating contractual requirements, and exposing the geographic location of individuals.**
Internal Use	Definition	Internal Use information is information originated or owned by your Company or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the your Company's business interests.
	Potential Impact of Loss	· **MINIMAL or NO DAMAGE would occur if Internal Use information were to become available to unauthorized parties either internal or external to your Company.** · **Impact could include damaging the your Company's reputation and violating contractual requirements.**
Public	Definition	Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.
	Potential Impact of Loss	· **NO DAMAGE would occur if Public information were to become available to parties either internal or external to your Company.** · Impact would not be damaging or a risk to business operations.

There are several types of assets in Information Security: Information, Software, Equipment, People, Facilities, Services. For SwiftCom Solutions, information asset is the critical one as organization is taking cloud services from third party and has relevant customers, employees and company data.

Assets in SwiftCom are broadly categorized as:

1. Asset name: Customer Data

ID	Name of Asset	Description of Asset	Type of Asset	Asset Owner (Accountable)	Classification	Location of Asset
1	Customer Data	PII, customer subscription plans, communication records	Information	Ethan Blake	Restricted	Cloud

Description: Customer's data will include PII (name, email, address, SIN, contact number), subscription plan, communication records.

Type of Asset: Information

Classification: Restricted

Location of Asset: Cloud

2. Asset Name: Employee Data

ID	Name of Asset	Description of Asset	Type of Asset	Asset Owner (Accountable)	Classification	Location of Asset
2	Employee Data	PII, Employment information (Salary, performance reviews)	Information	Ethan Blake	Confidential	Cloud

Description: Employee's record will include PII (name, address, email, SIN, contact number) and employment information (Salary, performance reviews, history of employment, benefits).

Type of Asset: Information

Classification: Confidential

Location of Asset: Cloud

3. Asset Name: Financial Records

ID	Name of Asset	Description of Asset	Type of Asset	Asset Owner (Accountable)	Classification	Location of Asset
3	Financial Records	Financial transactions, Budgets, Billing records	Information	Brett Kim	Restricted	On premises

Description: It includes financial transactions, budgets, billing records, and invoices.

Type of Asset: Information

Classification: Restricted

Location of Asset: On- premises

4. Asset Name: Intellectual Property

ID	Name of Asset	Description of Asset	Type of Asset	Asset Owner (Accountable)	Classification	Location of Asset
4	Intellectual Property	Software codes, algorithms, business development plans, research findings	Information	Isabella Khan	Confidential	On premises

Description: Trademarks, logos, branding materials, Patents and proprietary technology, Software code, and algorithms.

Type of Asset: Information

Classification: Confidential

Location of Asset: On - premises

8.3 Security Impact Analysis

It will assess the severity or harm to assets based on CIA as well as regulatory, reputational or financial security characters.

- Confidentiality: Prevents unauthorized access or disclosure to data.
- Integrity: Prevents unauthorized alteration of data.
- Availability: Ensures uninterrupted access to objects.
- Regulatory: Legal actions or legal proceedings.
- Reputational: Damage to company's reputation.
- Financial: Monetary fines.

Impact will be assessed on the factors:

- Very High: Fatal (critical)
- High: Vital (critical)
- Medium: Serious (non-critical)
- Low: Important (non-critical)
- Very Low: Non- important (non-critical)

Rate the Impact ⬇	Step 2: Impact Analysis - Asses the Severity or Harm to Assets Using these Information Security Characteristics					
	Cofidentiality (C) Unauthorized Use or Disclosure	**Integrity (I)** Unauthorized Destruction, Modification or Computation	**Availability (A)** System Failure or Inaccessibility	**Regulatory or Legal**	**Reputational**	**Financial (C$)**
Very High	Proprietary information (executive correspondence, financial statements, payroll information, etc.), trade secrets, operational processes, source code and technical information integral to the success of the company, and customer proprietary information (accounts and balances, financial statements, partnership agreements, contracts, etc.).	Modification Destruction or Corruption of: •Vital or mission critical information •Important research •Business plans or expansion plans •Personally identifiable information (PII) •Published financial statements contain critical material errors	•System failure causing catastrophic damage •Loss of a critical system, network or business application for an extended period of time affecting the entire organization	•Regulatory and/or legal action resulting in legal prosecution or suspension of operations	•Global damage to your Comany's reputation •Unsafe and unreliable operation	•Immediate revenue loss of > $500,000 •Cost Recovery > $500,000
High	Customer information (names, contacts, addresses, telephone numbers, electronic mail addresses, etc.), processing volumes, service pricing, equipment configurations, vendor information (names, addresses and telephone numbers), general employee information (name, home address, telephone number, years of service, etc.), application software used, and types and numbers of computer equipment.	Modification Destruction or Corruption of: •Important information •Important research •Personnel files (employees, contractors) •Regulatory filings contain significant material errors •Financial info resulting in incorrect payments to suppliers or partners	•System failure causing major damage •Loss of critical system, network or business application for an extended period of time affecting an entire department	•Regulatory and/or legal action resulting in fines or punitive action	•Local damage to your Comany's reputation •Reduction of safe & reliable operations	•Immediate revenue loss of < $500,000 •Cost Recovery <$500,000
Medium	General corporate information, employee names and their direct telephone numbers, facsimile telephone numbers, employee electronic mail addresses, facility addresses, total number of employees, or other high-level statistical information. Some high-level and general technical information can be included in this category as well.	Modification Destruction or Corruption of: •Internal company information •Intranet information is altered with incorrect information •Information or computing system tampering requiring moderate amount of time to recreate lost or corrupted information	•System failure causing moderate damage •Loss of an important system, network or business application affecting an entire department	•Regulatory and/or legal action resulting in administrative response	•Potential damage to your Comany's reputation •Safe operations of facilities	•Revenue loss increases with tim •Cost Recovery <$100,000
Low	Information that is public knowledge or readily available to the public. Unrestricted information may be disclosed in the normal course of conversation or other methods of communication. Information that is considered unrestricted includes, but is not limited to, publicly available sales and marketing materials and other information regarding products and services offered, general electronic mail addresses and general telephone numbers for voice or facsimile communication.	Modification Destruction or Corruption of: •Low value internal company information •Historical information is deleted •Information or computing system tampering requiring minimal amount of time to recreate lost or corrupted information	•Systems failure resulting in performance or functionality issues •Restricted access or loss of a system, network or business application for a temporary period	•No impact with regulatory or legal	•No reputation concerns •Safe operations	•No revenue loss •Cost Recovery <$25,000

1. Asset name: Customer Data

ID	Name of Asset	Confidentiality	Integrity	Availability	Regulatory	Reputational	Financial	Impact Rating	Impact Rating Averag
1	Customer Data	High	Very High	Very High	Very High	Very High	High	Very High	4.667

Average security impact rating = 4.667

2. Asset Name: Employee Data

ID	Name of Asset	Confidentiality	Integrity	Availability	Regulatory	Reputational	Financial	Impact Rating	Impact Rating Averag
2	Employee Data	Very High	Very High	High	High	High	High	High	4.333

Average security impact rating = 4.333

3. Asset Name: Financial Records

ID	Name of Asset	Confidentiality	Integrity	Availability	Regulatory	Reputational	Financial	Impact Rating	Impact Rating Averag
3	Financial Records	Very High	High	Medium	High	Very High	Low	High	3.833

Average security impact rating = 3.833

4. Asset Name: Intellectual Property

ID	Name of Asset	Confidentiality	Integrity	Availability	Regulatory	Reputational	Financial	Impact Rating	Impact Rating Averag
4	Intellectual Property	Very High	Very High	Medium	Low	Low	Low	Medium	3.167

Average security impact rating = 3.167

8.4 Threat Exposure (Risk) Rating

This stage will identify threats and how likely that threat will happen.

Ratings are classified into 5 ratings with values range from 0% to 100% with the description:

- Almost Certain: Value>90%, History of threat Event in SwiftCom and event is expected to occur.
- Likely: Value 51% - 90%, History of threat event in Swiftcom and event is likely to occur.
- Possible: Value 11% - 50%, Some history of threat event and there is a possibility that threat may occur.
- Unlikely: Value 4% - 10%, Limited evidence or history of threat event in SwiftCom and it is unlikely that threat will occur.
- Rare: Value < 3%, No evidence or history of threat and threat is highly unlikely to occur.

Rating	Likelihood Value	Frequency Description
Almost Certain	>90%	There is a history of threat events and a threat event is expected to occur
Likely	51 - 90%	There is a history of threat events and a threat event is likely to occur
Possible	11 - 50%	There is some history of threat events and there is a possibility a threat event may occur
Unlikely	4-10%	There is limited evidence or history of threat events involving the asset and the threat is considered unlikely to occur
Rare	< 3 %	There is NO evidence or history of threat events involving the asset and the threat is considered highly unlikely to occur

Determining threat exposure and rating

Impact X Likelihood		Organizational Impact Estimation (step 1)				
		Very High	High	Medium	Low	Very Low
Likelihood Rating (step 2)	Frequent	8	7	6	5	4
	Likely	7	6	5	4	3
	Possible	6	5	4	3	2
	Unlikely	5	4	3	2	1
	Highly Unlikely	4	3	2	1	0

Threat Exposure Rating	
Very High	8
High	6 - 7
Medium	4 - 5
Low	2 - 3
Very Low	0 - 1

1. Asset name: Customer Data

ID	Name of Asset	Threat Description	Threat Likelihood	Threat Exposure Rating	Threat Exposure Rating Number
1	Customer Data	Destruction of records	Likely	High	7

Threat Exposure rating: 7

Customer data is available on the cloud, the identified threat is “destruction of records” and there is 51% - 90% likelihood that a threat event can occur.

2. Asset Name: Employee Data

ID	Name of Asset	Threat Description	Threat Likelihood	Threat Exposure Rating	Threat Exposure Rating Number
2	Employee Data	Disclosure of information	Likely	High	6

Threat Exposure rating: 7

Similar to customer data, employee data is available on the cloud, the identified threat is “disclosure of information” and there is 51% - 90% likelihood that a threat event can occur.

3. Asset Name: Financial Records

ID	Name of Asset	Threat Description	Threat Likelihood	Threat Exposure Rating	Threat Exposure Rating Number
3	Financial Records	Unauthorized changes of records	Possible	Medium	5

Threat Exposure rating: 7

SwiftCom has kept its financial record in the headquarters which is on the premises, the identified threat is "unauthorized changes of records" and there is 11% - 50% likelihood that a threat event may occur.

4. Asset Name: Intellectual Property

ID	Name of Asset	Threat Description	Threat Likelihood	Threat Exposure Rating	Threat Exposure Rating Number
4	Intellectual Property	Industrial espionage	Likely	Medium	5

Threat Exposure rating: 7

Similar to financial records, Intellectual property is placed in the headquarters which is on the premises, the identified threat is "industrial espionage" and there is 51% - 90% likelihood that a threat event can occur.

9. Risk Management Strategy

9.1 Vulnerability Identification

In this section, vulnerabilities have been identified for the assets. Based on the threats that SwiftCom has on its assets, there is possibility of threat event to occur which depends on its weakness.

Vulnerability Severity Rating	Vulnerability Description
High	Vulnerabilities that allow an attacker immediate access into a system, elevated access or to bypass a security mechanism (i.e. firewall)
Medium	Vulnerabilities that provide information that have a high potential of granting unauthorized access
Low	Vulnerabilities that provide information, which when combined with other vulnerabilities could lead to compromise

1. Asset name: Customer Data

ID	Name of Asset	Vulnerability Description	Vulnerability Severity
1	Customer Data	Inadequate or irregular backup	Medium

- **Recognized threat:** Destruction of Records
- SwiftCom is not maintaining its regular backups which is scored as 1 out 4, so there are high chances of destruction of records.

2. Asset Name: Employee Data

ID	Name of Asset	Vulnerability Description	Vulnerability Severity
2	Employee Data	Lack of procedure for removing access rights upon termination of employment	Medium

- **Recognized threat:** Disclosure of Information
- There is no such record of information security policy that describes the responsibilities of employees after they have left the organization or changed their position internally. Information can be misused and there is lack of access rights.

3. Asset Name: Financial Records

ID	Name of Asset	Vulnerability Description	Vulnerability Severity
3	Financial Records	Too much power in one person	High

- **Recognized threat:** Unauthorized changes of records.
- These records are available on premises where too much power is given to one person only and that employee if not following the guidelines then can change the records.

4. Asset Name: Intellectual Property

ID	Name of Asset	Vulnerability Description	Vulnerability Severity
4	Intellectual Property	Inadequate control of physical access	Medium

- **Recognized threat:** Industrial Espionage
- Recently SwiftCom has faced a cyber-attack and there is a chance that there is a spy in the company who provides internal information externally. So for the IP of the company, there is need to keep it safe. Valid physical controls are available, the room is locked but information is available to unauthorized person who is authorized to get into the room.

9.2 Evaluation of Existing Safeguards and Residual Risk Ratings

As per ISO 27001: 2022, there are a few controls that SwiftCom needs to implement to enhance security.

Efficacy: Effectiveness, after implementing these safeguards, can be assessed in 4 ratings

- High: Safeguards are very effective and probability of compromise will be less than 10%.
- Medium: Safeguards will provide moderate effectiveness and the probability of compromise will be between 50% - 90%.
- Low: Safeguards will provide low effectiveness and the probability of compromise will be between 10% - 50%.
- None: Safeguards are ineffective and the probability of compromise will be greater than 90%.

Control Effectiveness	Description	Associated Attributes	Outcome
High	**Safeguards Very Effective** Probability of Compromise < 10%	• Difficult to exploit • Requires extensive knowledge & skills to exploit • Access to assets tightly controlled • Staff well-informed and trained	• Compromise almost certainly detected quickly • Damage tightly contained • Quick and complete recovery
Medium	**Moderate Safeguards Effectiveness** Probability of Compromise 50-90%	• Not easily exploited • Requires some knowledge & skills to exploit • Assets moderately accessible • Moderate staff awareness and training	• Compromise probably detected over time • Damage partially contained • Moderate recovery times/ • Service levels exist
Low	**Low Safeguards Effectiveness** Probability of Compromise 10-50%	• Possible to exploit • Requires little knowledge & skills to exploit • Assets easily accessible • Staff ill-informed and poorly trained	• Unlikely to detect compromise • Damage difficult to contain • Prolonged recovery times • poor service levels
None	**Safeguards Ineffective** Probability of Compromise > 90%	• Very Easily exploited • Requires little knowledge & skills to exploit • Assets highly accessible • Staff ill-informed and not trained	• Unlikely to detect compromise • Unable to contain damage • Prolonged recovery time • No service levels

Residual risk: The risk that remains after efforts to identify and eliminate some or all types of risk have been made.

Low or Very Low (1-2)	Medium (2)	High (4)	Very High (5)
Residual risk not reported.	Residual risk reported to: • Asset Owner • Dept Head • VP	Residual risk reported to: • Asset Owner • Dept Head • MRU ERM Steering Committee • CIO • AVP	Residual risk reported to • Asset Owner • Dept Head • MRU ERM Steering Committee • CIO, AVP • President
Some residual risk controls/mitigation measures may be required or known residual risk is accepted.	Key controls and/or Management activities in place, with opportunities for improvement identified.	Limited or non-existent controls and/or Management activities in place, high level of risk remains.	Limited or non-existent controls and/or Management activities in place, high level of risk remains.
Residual risk will not be tracked in Risk Register.	Residual risk will be tracked in Risk Register.	Residual risk will be tracked in Risk Register.	Residual risk will be tracked in Risk Register.
No Opportunity for Improvement	Limited Opportunity for Improvement	Moderate Opportunity for Improvement	Significant Opportunity for Improvement
Corrective actions may not be justifiable or cost effective.	Corrective actions are needed, and a risk mitigation treatment plan must be developed to address risk in a reasonable time frame.	Corrective actions are needed, and a risk mitigation treatment plan must be developed to address risk as soon as possible.	Corrective actions are needed, and a risk mitigation treatment plan must be developed to address risk immediately.
No further mitigation required.	No further mitigation required where controls are verified to be working as intended.	CIO approval prior to implementation or continued operation of the solution unless an exemption is obtained.	CIO approval prior to implementation or continued operation of the solution unless an exemption is obtained.

Determining Residual risk rating

Safeguard Effectiveness (# 6) ➡	NONE	LOW	MED	HIGH	NONE	LOW	MED	HIGH	NONE	LOW	MED	HIGH
Vulnerability Severity (# 5) ➡	HIGH				MEDIUM				LOW			
Threat Exposure Rating (# 4) ⬇	Residual Risk Rating ⬇				Residual Risk Rating ⬇				Residual Risk Rating ⬇			
Very High	5	5	4	4	5	4	4	3	4	4	3	3
High	5	4	4	3	4	4	3	3	4	3	3	2
Medium	4	4	3	3	4	3	3	2	3	3	2	2
Low	4	3	3	2	3	3	2	2	3	2	2	1
Very Low	3	3	2	1	3	2	2	1	2	2	1	1

1. Asset name: Customer Data

ID	Name of Asset	Primary Safeguard	Primary Safegaurd ID	Primary Safeguard Rating	Secondary Safegaurd 1	Secondary Safegaurd 2	Residual Risk Rating	Residual Risk Number
1	Customer Data	12.3.1 Information back-up	ISO-062	High	18.1.4 Privacy and protection of personally identifiable	18.1.3 Protection of Corporate records	Medium	3

- Primary safeguard: Information back-up (ISO 8.13)
- Secondary safeguard: Privacy and protection of PII (ISO 5.34), Protection of Corporate records (ISO 5.33).
- **Residual risk rating:** Medium

2. Asset Name: Employee Data

ID	Name of Asset	Primary Safeguard	Primary Safegaurd ID	Primary Safeguard Rating	Secondary Safegaurd 1	Secondary Safegaurd 2	Residual Risk Rating	Residual Risk Number
2	Employee Data	7.3.1 Termination or change of employment responsibilities	ISO-015	High	7.1.2 Terms and conditions of employment	7.2.2 Information security awareness, education and training	Medium	3

- Primary safeguard: Termination or change of employment responsibilities (ISO 6.5).
- Secondary safeguard: Terms and conditions of employment (ISO 6.2), Information Security awareness, education and training (ISO 6.3).
- **Residual risk rating:** Medium

3. Asset Name: Financial Records

ID	Name of Asset	Primary Safeguard	Primary Safegaurd ID	Primary Safeguard Rating	Secondary Safegaurd 1	Secondary Safegaurd 2	Residual Risk Rating	Residual Risk Number
3	Financial Records	9.2.6 Removal or adjustment of access rights	ISO-033	Medium	9.2.5 Review of user access rights	9.2.2 User access provisioning	Medium	3

- Primary safeguard: Removal or adjustment of access rights (ISO 5.18).
- Secondary safeguard: Review of user access rights (ISO 5.18), User access provisioning (ISO 5.18).
- **Residual risk rating:** Medium

4. Asset Name: Intellectual Property

ID	Name of Asset	Primary Safeguard	Primary Safeguard ID	Primary Safeguard Rating	Secondary Safeguard 1	Secondary Safeguard 2	Residual Risk Rating	Residual Risk Number
4	Intellectual Property	11.1.3 Securing offices, rooms and facilities	ISO-044	High	11.1.2 Physical entry controls	11.1.5 Working in secure areas	Low	2

- Primary safeguard: Securing offices, rooms and facilities (ISO 7.3)
- Secondary safeguard: Physical entry controls (ISO 7.2), working in secure areas (ISO 7.6).
- **Residual risk rating:** Low

Determine risk treatment by existing residual risk rating

Based on the Residual Risk Rating, risk treatment will be determined, and Risk Decisions will be made. The following table will be used as guidance for determining the appropriate course of action commensurate with the level of Residual Risk.

Residual Risk Options				
Residual Risk Rating	**Low / Very Low (1-2)**	**Medium (2)**	**High (4)**	**Very High (5)**
Existing *(Residual)* **Risk Status** *including safeguards and opportunity for improvement*	Existing Safeguards High\y Effective. Limited insignificant residual risk remains. Controls or mitigation measures may be required or can be easily accepted. No Opportunity for Improvement	Moderate Effectiveness of Existing Safeguards. Key security controls and/or Management activities in place, with opportunities for improvement identified, some risk remains. Limited Opportunity for Improvement	Low Effectiveness of Existing Safeguards. Limited controls and/or Management activities in place, high level of risk remains. Moderate Opportunity for Improvement	Existing Safeguards Ineffective. Limited or non-existent security controls and/or Management activities in place, very high level of risk remains. Significant Opportunity for Improvement
Risk Treatment Process				
Risk Treatment Options *(for Asset Owner)*	Available risk treatment options for Asset Owner: • Accept. • Reduce • Avoid • Transfer	Available risk treatment options for Asset Owner: • Accept. • Reduce • Avoid • Transfer	Available risk treatment options for Asset Owner: • Accept. • Reduce • Avoid • Transfer	Available risk treatment options for Asset Owner: • Accept. • Reduce • Avoid • Transfer
Corrective Action	Corrective actions may not be justifiable or cost effective.	Corrective actions are needed, and a risk mitigation treatment plan may be needed to address risk in a reasonable time frame.	Corrective actions are needed, and a risk mitigation treatment plan must be developed to address risk as soon as possible.	Corrective actions are needed, and a risk mitigation treatment plan must be developed to address risk immediately.
Reporting	Residual risk not reported .	Residual risk reported to: • Asset Owner(s) • Dept Head • VP • Compliance Dept.	Residual risk reported to: • Asset Owner(s) • Dept Head • Compliance Dept. • VP level • Enterprise Risk Management • CIO / CISO	Residual risk reported to: • Asset Owner(s) • Dept Head • Compliance Dept. • Enterprise Risk Management • VP Level • CIO / CISO • President / CEO • Board of Directors
Risk Register	Residual risk will not be tracked in Risk Register.	Residual risk will be tracked in Risk Register.	Residual risk will be tracked in Risk Register.	Residual risk will be tracked in Risk Register.
Approvals to Proceed & Next Steps	No further mitigation required.	No approvals required where controls are verified to be working as intended.	Appropriate approval required prior to implementation or continued operation of the asset/solution unless an exemption is obtained.	Appropriate approval required prior to implementation or continued operation of the asset/solution unless an exemption is obtained.

9.3 Maintaining the Risk Register

The risk assessment and available risk treatment options will be discussed with the asset owner. Once a decision has been established, a recommended course of action for each residual risk to be addressed and update the risk register.

IT Risk Register

ID	Name of Asset	Description of Asset	Asset Owner (Accountable)	Classification	Security Impact Rating	Threat Description	Threat Exposure Rating	Vulnerability Description	Vulnerability Severity	Existing Safeguard Description	Existing Safeguard Effectiveness	Residual Risk Rating (Priority Level)	Risk Decision	Risk Owner	Start Date	Due Date
#	*From Risk Assessment*	*From Risk Assessment*	*From Risk Assessment*	*From Risk Assessment*	*From Risk Assessment (includes Confidentiality, Integrity,*	*From Risk Assessment*	*From Risk Assessment (includes*	*From Risk Assessment*	*From Risk Assessment*	*From Risk Assessment*	*From Risk Assessment*	*From Risk Assessment*	*Risk treatment options for Asset*	*Who is accountable for the risk?*	*Date risk treatment commenced*	*Projected date of risk treatment completion*
1	Customer Data	PII, customer subscription plans,	Ethan Blake	Restricted	Very High	Destruction of records	High	Inadequate or irregular backup	Medium	12.3.1 Information back-up	High	Medium	REDUCE	Ethan Blake	5/1/2024	8/31/2024
2	Employee Data	information (Salary, performance reviews)	Ethan Blake	Confidential	High	Disclosure of Information	High	Lack of procedure for removing access rights upon termination of employment	Medium	7.3.1 Termination or change of employment responsibilities	High	Medium	REDUCE	Ethan Blake	5/1/2024	11/1/2024
3	Financial Records	transactions, Budgets, Billing records	Brett Kim	Restricted	High	Unauthorized changes of records	Medium	Too much power in one person	High	9.2.6 Removal or adjustment of access rights	Medium	Medium	REDUCE	Brett Kim	4/1/2024	6/31/2024
4	Intellectual Property	Software codes, algorithms,	Isabella Khan	Confidential	Medium	Industrial Espionage	Medium	Inadequate control of physical access	Medium	11.1.3 Securing offices, rooms and facilities	High	Low	REDUCE	Isabella Khan	6/1/2024	12/31/2024

10. Concluding Remarks

In conclusion, SwiftCom's overall security posture is improved but there are a few improvements that need to be made. Making a strategy for cybersecurity, improving six priority focus areas, hiring for new positions, using regulations like COBIT, CRTC, and standardization such as ISO 27001, ISO 37001, performing security control gap assessment and risk assessment, applying security controls and making decisions for the risks such as accept, mitigate, avoid, transfer.

11. Document History

VERSION	DATE	AUTHOR	DESCRIPTION OF REVISIONS
0.01	March 11, 2024	Meenu Handa	Initial draft
0.02	March 31, 2024	Meenu Handa	Amendments
0.03	April 04, 2024	Meenu Handa	Final Draft

12. References

[1] Dan Blum (2020), *"Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment"*, Apress Open

[2] Service Alberta and the Office of the Information and Privacy Commissioner (2008), *"A Guide for Businesses and Organizations on the Personal Information Protection Act"*, https://www.oipc.ab.ca/wp-content/uploads/2022/02/PIPA-Guide-2008.pdf

[3] Open Media (June 28, 2022), *"What is the CRTC? And why should I care?"*, https://openmedia.org/article/item/crtc-faq

[4] Katie Terrell Hanna (September 2021), *"What is COBIT (Control Objectives for Information and Related Technologies)?"*, https://www.techtarget.com/searchsecurity/definition/COBIT#:~:text=COBIT%20is%20an%20IT%20governance,for%20Information%20and%20Related%20Technologies.

[5] Christophe Veltsos (February 8, 2017), *"NACD Publishes Five Cybersecurity Principles Every Board Director Needs to Know",* https://securityintelligence.com/nacd-publishes-five-cybersecurity-principles-every-board-director-needs-to-know/
[6] Susan Moore, Gartner (July 2019), *"Keep Your Job After a Cyberattack"*, www.gartner.com/smarterwithgartner/keep-your-job-after-a-cyberattack/

13. List of Attached Appendices

Term	Definition
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Integrity	A property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored.
Availability	Timely, reliable access to data and information services for authorized users.
Risk	A measure of the likelihood and the consequence of events or acts that could cause a system compromise, including the unauthorized disclosure, destruction, removal, modification, or interruption of system assets.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.
Asset	Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards).
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Impact	The effect on organizational operations, organizational assets, individuals, or the Nation of a loss of confidentiality, integrity, or availability of information or an information system.
Residual Risk	The potential for the occurrence of an adverse event after adjusting for the impact of all in-place safeguards.
Risk Treatment	Process to modify risk.
Risk Register	A central record of current risks, and related information, for a given scope or organization.