Cybersecurity Business Plan

developed for

Firearm Corporationon

April 18th, 2024

Developed by Sarah Syeda, Director of Cybersecurity

Table of Contents

Company Introduction

FireArm Security Solutions, stands at the forefront of safeguarding what matters most; security, assets, and peace of mind. As a premier provider of private security services, the company specializes in protecting executives, government officials, and ensuring comprehensive site surveillance.

FireArm Security Solutions traces its roots back to the vibrant city of Calgary, Alberta, where it was established in 1995 by two former law enforcement officers, James McAllister and Sarah Nguyen. Both shared a vision of creating a security company that would redefine the standards of protection and professionalism in the industry. FireArm invested heavily in cutting-edge technology and ongoing training for its personnel. The company became a pioneer in the use of advanced surveillance systems, threat detection software, and tactical training programs, ensuring that its clients received the highest level of protection available.

Mission

To empower clients with the highest level of security solutions, tailored to their unique needs. We believe that every individual and organization deserves the assurance of safety and confidentiality, and we make it our mission to deliver exactly that.

The business

At FireArm, we are more than a security company; we are your trusted partners in fortifying your defenses against threats, both seen and unseen.

Executive Protection: Our elite team of security experts provides discreet and reliable protection for high-profile individuals, ensuring their safety in every scenario.

Government Officials Security: We understand the unique challenges faced by government officials. Our specialized services offer comprehensive protection, safeguarding personal information and ensuring secure environments.

Site Surveillance Solutions: From corporate offices to remote locations, we deploy advanced surveillance systems and expert personnel to monitor, detect, and deter threats effectively.

How the business works

Tailored Solutions: No two security needs are alike. That's why we take a personalized approach to every client engagement, conducting thorough assessments to understand your risks and requirements.

Proactive Security: Anticipation is key to effective security. We stay ahead of the curve by continuously monitoring trends, updating protocols, and leveraging the latest technologies.

Ethical Practices: Integrity is the cornerstone of our operations. We adhere to the highest ethical standards, ensuring transparency, confidentiality, and trust in all our dealings.

Executive Overview

THE BREACH

Risk:
Recently, the company experienced a significant data breach resulting in the leak of sensitive customer information, including personal identifiable information of government officials.

Impact and Accountability:
This breach discovered in December, 2023 has raised concerns about corporate espionage and insider threats. The breach incurred a cumulative monetary loss of approximately $8 million directly attributed to the data breach. This includes revenue from lost contracts, legal and regulatory expenses, remediation costs, client fallout, and reputational damage. As a result, FireArm has had their government clearance revoked until their management team has demonstrated a remediation roadmap in their information security program

Cause:
Security auditors have completed an assessment and have presented their report. They discovered the cause of the breach was executed malware on a USB key using a contractor's credentials to gain access to the company's network and sensitive data. Auditors noted a lack of a formal information security program, limited controls to prevent non-IT personnel from installing software and no controls for USB storage media.

THE PROCESS

Actionable improvement objectives:

In response, FireArm has developed a comprehensive cybersecurity business plan to remediate the breach, regain government clearance, and fortify its information security posture. The plan includes getting 95% of the benefit expected from a security program for 5% of the work. In order to do that, we align the business on the core Rational Cybersecurity pareto priority areas, that are:

1. Risk management,
2. Control baseline,
3. Security culture,
4. IT rationalization,
5. Access control, and
6. Cyber-resilience

Assessing Current Security Posture:

1. Gap Assessment: Identifying gaps in controls and procedures against ISO 27002.
2. Threat Risk Assessment (TRA) with ISO 27005 to analyze threats, vulnerabilities, and impacts on information assets.

Management support:
Business executives will work in good faith for the good of the business, so that the efforts of the cybersecurity team will eventually be rewarded with understanding and acceptance. The CISOs on the other hand will function as business leaders for their security teams, in order to engage and align with the business at all levels

THE SCALABLITIY

FireArm recognizes the critical importance of scalability in its cybersecurity initiatives, tailored to the unique aspects of its organization:

Size of the Organization: As a medium-sized company poised for growth, FireArm will ensure that its security programs are scalable to accommodate an expanding client base and workforce.

Complexity of IT Infrastructure: With diverse systems and networks, including cloud-based services and on-premises solutions, FireArm's security measures will be designed to be scalable without compromising efficiency.

Security Pressure: Following the breach and the revocation of government clearance, FireArm has faced heightened security pressure. Hence, scalable security programs are crucial to adapt to evolving threats and compliance requirements.

National and Industry Origins: Operating in Canada's private security sector, FireArm will adhere to national cybersecurity standards while also considering industry-specific regulations. We believe that scalable programs are essential to remain compliant and competitive.

Security-Relevant Organizational Issues

Post the data breach, security auditors have completed an assessment and have presented their report. Auditors noted:

- A lack of a formal information security program.
- Limited controls to prevent non-IT personnel from installing software and no controls for USB storage media.

From the gap assessments, we are also lacking controls in few other domains. These domains include:

- Organization of Information Security
- Access Controls
- Asset Management
- Physical and Environmental Security

On performing research on the organizations operating in the same area as ours, some of the findings show, similar breaches occurred in the past to our rivalries. Approximately a 30M $ was lost due to these breaches. Post the breach, many organization-initiated process to become ISO certified and started to see their security posture to be above average/good. Currently, we are not complaint with ISO.

Cybersecurity Strategy

Area of Focus

Primary Business Goals:

1. Client Satisfaction and Safety:

- Ensure the safety and security of clients, including executives and government officials, through effective security measures and surveillance.
- Provide reliable and responsive security services to meet client needs and expectations.

2. Government Contracts and Partnerships:

- Secure and maintain government contracts by demonstrating excellence in security services and adherence to government standards.
- Establish strong partnerships with government agencies to become a trusted provider of security solutions.

3. Risk Mitigation and Threat Prevention:

- Proactively identify and mitigate security risks, including cyber threats, physical intrusions, and unauthorized access.
- Implement robust security protocols to prevent security breaches and incidents.

4. Compliance with Regulations:

- Ensure strict compliance with industry-specific regulations, government security standards, and data protection laws.
- Maintain certifications and accreditations necessary for providing security services to government and private sector clients.

5. Operational Efficiency and Effectiveness:

- Streamline operational processes to deliver cost-effective security solutions without compromising quality.
- Optimize resource allocation and staffing to enhance service delivery and response times.

Secondary Business Goals:

1. Market Expansion and Growth:

- Explore opportunities for expanding services into new markets, both geographically and within different sectors.
- Develop targeted marketing strategies to attract new clients and increase market share.

2. Technology Integration and Innovation:

- Incorporate advanced technologies such as AI-driven surveillance systems, biometric access controls, and cybersecurity solutions.
- Foster a culture of innovation to continuously improve security services and stay ahead of emerging threats.

3. Employee Training and Development:

- Invest in ongoing training programs for security personnel to enhance skills in threat detection, crisis management, and client interaction.
- Promote a culture of professionalism and excellence to build a skilled and motivated workforce.

4. Brand Reputation and Trust:

- Build a strong brand reputation as a reliable and trustworthy security provider in the industry.
- Leverage client testimonials, case studies, and successful project outcomes to enhance credibility.

Relevant Corporate and IT Strategies:

1. Corporate Strategy:

- Focus on customer-centricity, ensuring that all security solutions are tailored to meet client needs and exceed expectations.
- Emphasize a culture of compliance, with regular audits and assessments to maintain adherence to regulations and standards.

2. IT Strategy:

- Invest in state-of-the-art cybersecurity technologies to protect client data, prevent breaches, and ensure data integrity.
- Implement a robust incident response plan, including regular drills and simulations, to effectively manage security incidents.
- Integrate security systems with IoT devices and cloud platforms for real-time monitoring and remote access.
- Develop a scalable IT infrastructure to support business growth and the adoption of new technologies.

Company-Specific Security Goals

I. Develop and Govern a Healthy Business Culture

Address Common Challenges:

1. Business Executives Not Engaged at the Strategic Level
   - Executive Training Initiative: Launch a specialized cybersecurity training program for executives, tailored to the unique challenges and security requirements of the private security industry.
   - Strategic Alignment Campaign: Initiate a campaign to promote cybersecurity as a strategic priority within FIREARM, emphasizing its role in safeguarding sensitive client information and maintaining the company's competitive edge.
   - Cybersecurity Risk Assessment: Conduct a thorough assessment of cybersecurity risks specific to FIREARM's operations, including potential threats to executive protection services and site surveillance operations.
   - Executive Engagement Sessions: Organize regular executive briefings and workshops to foster open dialogue and engagement between cybersecurity experts and senior leadership, ensuring that security concerns are addressed at the highest levels of the organization.

2. Business Units at Odds with IT and Security

In FIREARM Security Solutions, potential conflicts between business units and IT (including security) may arise due to various factors inherent in our industry and organizational structure. The high-stakes nature of our security services, catering to executives and government officials, often prioritizes immediate client needs over IT and security considerations. Additionally, the sensitive nature of our operations demands strict adherence to regulations and protocols, sometimes leading to friction between business units seeking flexibility and IT/security teams enforcing compliance. The rapid advancements in security technologies and the evolving threat landscape pose ongoing challenges for aligning business objectives with IT and security strategies. For example, as we embrace cutting-edge surveillance technologies and biometric access controls, there may be resistance from business units accustomed to traditional security measures. Moreover, our expansion into new markets and partnerships may introduce complexities in IT infrastructure management and data protection, further complicating the relationship between business units and IT/security functions.

In certain scenarios within FIREARM, IT and security teams may align with the trend towards cloud-first strategies, leveraging cloud-based platforms for data storage and collaboration. However, the unique requirements of our security operations, such as the need for offline data storage and restricted access to sensitive information, may pose challenges to fully embracing cloud technologies. Perceptions of inefficiency or resistance from central IT or security can erode trust and collaboration within our organization. For instance, delays in deploying security updates or a perceived lack of responsiveness to urgent security threats can strain relationships between business units and IT/security teams. Additionally, if security leaders are perceived as overly restrictive or fail to understand the operational realities faced by frontline security personnel, morale and productivity may be affected.

In FIREARM, where our operations span across different regions and cultures, ensuring effective communication and alignment between business units and central IT/security functions becomes even more crucial. Misunderstandings or misinterpretations of security policies and procedures can lead to compliance gaps and security vulnerabilities, posing significant risks to our organization's reputation and operations.

To address these challenges, FIREARM Security Solutions must prioritize open communication, collaboration, and mutual understanding between business units and IT/security teams. By fostering a culture of transparency and empathy, providing tailored solutions that balance security requirements with operational needs, and investing in ongoing training and development for all stakeholders, we can strengthen our organization's security posture and resilience against emerging threats.

Security Governance Improvement Objectivess	Security Culture Improvement Objectives
Enhance Security Policy Framework	Coordinate with the marketing organization's internal communications program. Increase Employee Awareness and Training
Implement Robust Risk Management Processes	Promote a Culture of Accountability and Reporting
Strengthen Security Awareness and Training Programs	Embed Security into Organizational Values and Practices

II. Manage IT Risk in the Language of Business

Educate the Business on Risks to Avoid:

At FIREARM Security Solutions, our paramount goal is to mitigate IT risk in a manner that aligns with the unique needs and challenges of our industry. As a provider of private security services for high-profile individuals and government officials, we prioritize the protection of sensitive information and the integrity of our security operations. For instance, when evaluating potential technology partners or service providers, such as surveillance equipment manufacturers or software vendors, we place a strong emphasis on security and reliability. In accordance with our commitment to safeguarding client confidentiality, we may opt to avoid partnerships with vendors that lack robust security measures or have a history of data breaches. Educating our business leaders, IT professionals, and security personnel on the intricacies of risk management is essential to our success. By conducting regular training sessions and workshops, we ensure that all stakeholders are equipped with the knowledge and tools necessary to identify and address security risks effectively.

Furthermore, our security processes enable us to provide alternative solutions in instances where risk levels are deemed unacceptable. For example, if a proposed technology solution presents a high risk of data compromise, our security team can collaborate with business leaders to explore alternative vendors or implement additional security controls to mitigate the risk.

By managing IT risk in a language that resonates with our business objectives and values, FIREARM Security Solutions strengthens its position as a trusted leader in the security industry, ensuring the continued safety and satisfaction of our clients.

Share Responsibility, Outsource, or Obtain Insurance to Transfer Risk:

Given the nature of our business, transferring risk to a third party isn't always feasible due to the sensitive nature of our operations. However, we adopt a customized approach that involves sharing responsibilities, outsourcing certain security functions to trusted partners, and obtaining specialized insurance coverage to mitigate potential risks specific to our industry.
Strategic Partnerships: Collaborating with reputable security firms and technology providers allows us to share the responsibility of managing IT risk effectively. By leveraging their expertise and resources, we can enhance our security posture and address emerging threats more comprehensively.
Specialized Insurance Coverage: In addition to standard business insurance policies, we explore specialized cyber-insurance options tailored to the security industry. This coverage provides financial protection

against cybersecurity incidents, including data breaches, system outages, and legal liabilities arising from security breaches or operational disruptions.

III. Establish a Control Baseline

1. Risk Management:

- Establish a taxonomy framework and robust processes to identify, assess, mitigate, and monitor security risks associated with our operations.
- Ensure proactive communication and reporting of risks to relevant stakeholders, including clients and regulatory bodies.

2. Discovery and Classification:

- Implement inventory procedures to discover all firearms owned and utilized by the security personnel.
- Classify firearms based on their type, make, model, and serial number for accurate tracking and identification.

3. Security Policies and Awareness:

- Conduct regular security awareness training sessions to educate employees and contractors on security best practices and foster a culture of security awareness.

4. Network Security and Zoning:

- Implement network segmentation and zoning strategies to protect sensitive information and critical systems from unauthorized access.

5. Risk Profiling:

- Profile the risks associated with the possession and use of firearms, considering factors such as regulatory compliance, safety protocols, and training requirements.
- Assess the potential impact of firearm-related incidents on the security operations and reputation of the organization.

6. Critical Asset Identification:

- Identify firearms deemed critical for ensuring the safety and protection of clients, including government officials and executives.
- Assign ownership and responsibility for safeguarding critical firearms to designated asset owners within the organization.

7. Asset Owners and Responsibilities:

- Designate security personnel, such as team leaders or armory managers, as asset owners responsible for the maintenance, storage, and accountability of firearms.
- Define clear procedures and protocols for issuing, returning, and maintaining firearms in accordance with security policies and regulations.

8. Regulatory Compliance:

- Ensure compliance with relevant laws, regulations, and licensing requirements governing the possession, storage, and use of firearms.
- Maintain accurate records of firearm ownership, transfers, and usage to demonstrate compliance during audits and inspections.

9. Training and Certification:

- Provide comprehensive training programs for security personnel on the safe handling, operation, and maintenance of firearms.
- Ensure that security personnel possess the necessary certifications and qualifications to carry and use firearms in accordance with legal and industry standards.

10. Security Controls:

- Implement physical security measures, such as secure storage facilities and access controls, to prevent unauthorized access to firearms.
- Conduct regular audits and inventory checks to verify the accuracy and completeness of firearm records and holdings.

11. Incident Response, Logging and Reporting:

- Develop protocols for responding to firearm-related incidents, including accidents, loss, theft, or misuse.
- Establish reporting mechanisms for documenting and investigating firearm incidents, ensuring prompt notification to appropriate authorities and stakeholders.

IV. Simplify and Rationalize IT and Security

1. Streamline Firearm Infrastructure: We will streamline and modernize our IT infrastructure to better serve the needs of our security operations. This includes upgrading our surveillance systems, enhancing access control mechanisms, and optimizing our communication networks to ensure seamless coordination among our security personnel.

2. Optimize Security Applications: We will assess and rationalize our security application portfolios to ensure they are aligned with our operational requirements. This involves evaluating the effectiveness of our security tools, retiring outdated systems, and investing in cutting-edge technologies to bolster our defense capabilities.

3. Embrace Cloud Security Solutions: We will embrace cloud computing solutions tailored to the security industry, transitioning from traditional security models to cloud-based platforms. This shift will enable us to enhance scalability, improve data accessibility, and strengthen our incident response capabilities while maintaining stringent security measures.

4. Enhance Business Agility and Efficiency: Our strategy will focus on enhancing business agility and operational efficiency while minimizing security risks. We will collaborate closely with our IT and digital innovation teams to implement agile methodologies and streamline processes, enabling us to respond swiftly to emerging threats and client requirements.

5. Champion Best Practices: We will champion industry best practices in security, advocating for rigorous risk assessments, robust third-party risk management protocols, and the integration of security principles into our development processes. By showcasing these best practices, we aim to elevate our security standards and instill confidence in our clients.

6.Foster Interdepartmental Collaboration: Leveraging our cross-functional role, we will foster collaboration between our security, IT, and digital innovation teams. This collaboration will facilitate the exchange of insights, enable proactive problem-solving, and drive continuous improvement in our security posture.

V. Control Access with Minimum Drag on Business

For FIREARM Security Solutions, access control is not just a security measure; it's a fundamental aspect of ensuring the safety and confidentiality of our clients' information and operations. Our access control policies and procedures are meticulously designed to strike a balance between stringent security measures and the seamless execution of our security services.

In the realm of private security services for executives and government officials, access control is especially critical. We must ensure that only authorized personnel have access to sensitive information, surveillance systems, and security protocols. This includes restricting access to confidential client data, classified information, and critical infrastructure.

Our Identity and Access Management (IAM) practices are tailored to meet the unique needs of our industry. We employ advanced authentication and authorization mechanisms to verify the identities of our security personnel, ensuring that only qualified individuals are granted access to high-security areas and client information.

Furthermore, our access governance framework encompasses data protection disciplines such as information classification and data governance. We classify client data based on its sensitivity and implement appropriate access controls to safeguard against unauthorized disclosure or tampering.

In the fast-paced world of security operations, where every second counts, our access control measures are designed to minimize drag on business operations. We prioritize user-friendly authentication methods and streamline access approval processes to ensure that our security personnel can quickly respond to emerging threats and security incidents.

At FIREARM, we understand the delicate balance between security and operational efficiency. While access control is paramount for safeguarding our clients and their assets, we are committed to implementing measures that enable us to deliver agile and flexible security services without compromising on safety or privacy.

The improvement objectives we have identified are:

1. Conduct a rapid security assessment focused on IAM and data governance. Upgrade Salesforce to Implement Fine-Grained Access Controls Based on Role and Need-to-Know
2. Use the business impact assessment (BIA), the enterprise risk map, or other sources to find critical assets and risk owners. Automate Identity Lifecycle Management Processes
3. Enhance Identity Verification and Authentication Mechanisms

In essence, access control at FIREARM Security Solutions is not just about restricting access; it's about empowering our security personnel to fulfill their duties effectively while upholding the highest standards of confidentiality and integrity in everything we do.

VI. Institute Resilient Detection and Response

1. Identify Critical Assets and Risk Scenarios:

We meticulously identify critical assets, such as our executive protection databases, surveillance systems, and government liaison networks, to prioritize our protection efforts.
By conducting thorough risk assessments, including potential scenarios like targeted attacks on high-profile clients or breaches in sensitive government information, we tailor our security measures to effectively mitigate these specific threats.

2. Enhance Detection Capabilities:

Leveraging cutting-edge technology and expert analysis, to enhance our detection capabilities to identify suspicious activities or anomalies within our networks and systems.
Use advanced monitoring tools and threat intelligence integration to stay ahead of potential threats, ensuring early detection and response to any security incidents.

3. Strengthen Incident Response Coordination:

Create a dedicated Incident Response team, comprising security experts, legal advisors, and operational personnel, to ensure seamless coordination in response to security incidents.
Through regular training and simulation exercises, we must prepare our teams to swiftly respond to various scenarios, including cyber-attacks targeting our critical infrastructure or data breaches compromising client information.

4. Implement Structured Response Procedures:

In the event of a security incident, our response follows a structured and well-defined protocol, with each department having predefined roles and responsibilities.
Whether it's restoring affected systems, managing communications with clients and stakeholders, or coordinating with law enforcement, our response is swift, coordinated, and effective.

5. Develop Business Continuity Plans:

We conduct thorough assessments to identify potential disruptions to our operations and develop comprehensive business continuity plans.
These plans outline procedures for maintaining essential services, ensuring uninterrupted operations even in the face of severe incidents or emergencies.

6. Coordinate Recovery Efforts:

Our business continuity and incident response teams work hand-in-hand to coordinate recovery efforts, focusing on restoring critical services and mitigating the impact of incidents.
Whether it's recovering from a cyber-attack or mitigating the effects of a physical security breach, our teams collaborate seamlessly to minimize disruption and ensure business continuity.

Goal Timelines and Success Metrics

1. Develop and Govern a Healthy Business Culture:

Goal Timeline:
Year 1: Conduct culture assessments and surveys to understand current organizational culture.
Year 2: Develop and implement initiatives to promote a healthy work environment and values alignment.
Year 3: Monitor and evaluate progress, making adjustments as needed to sustain a positive culture.

Success Metrics:
Employee satisfaction survey results showing improvement in morale and engagement.
Decrease in turnover rates and increase in employee retention.
Positive feedback from employees on company culture initiatives and programs.

2. Manage IT Risk in the Language of Business:

Goal Timeline:
Year 1: Conduct IT risk assessments and identify key risk areas impacting business objectives.
Year 2: Develop risk management strategies aligned with business priorities and risk appetite.
Year 3: Implement risk mitigation measures and establish regular monitoring and reporting processes.

Success Metrics:
Reduction in the number of high-risk IT incidents impacting business operations.
Alignment of IT risk management practices with overall business strategy.
Compliance with regulatory requirements related to IT risk management.

3. Establish a Control Baseline:

Goal Timeline:
Year 1: Conduct comprehensive security assessments to identify existing controls and gaps.
Year 2: Develop and document a baseline of security controls aligned with industry standards and best practices.
Year 3: Implement control enhancements and establish a process for ongoing control monitoring and updates.

Success Metrics:
Completion of security control documentation and alignment with relevant frameworks (e.g., ISO 27001, NIST Cybersecurity Framework).
Reduction in the number of security incidents attributable to control deficiencies.
Positive feedback from auditors and regulators on the effectiveness of implemented controls.

4. Simplify and Rationalize IT and Security:

Goal Timeline:
Year 1: Conduct a comprehensive assessment of IT and security infrastructure, processes, and tools.
Year 2: Identify opportunities to streamline and simplify IT and security operations, eliminating redundancies and inefficiencies.
Year 3: Implement simplification initiatives and monitor their impact on operational effectiveness and agility.

Success Metrics:
Reduction in the number of IT and security tools and systems, with a focus on consolidation and integration.
Improvement in IT and security operational efficiency metrics (e.g., mean time to resolution, incident response times).
Positive feedback from IT and security teams on the ease of use and effectiveness of simplified processes and tools.

5. Control Access with Minimum Drag on Business:

Goal Timeline:
Year 1: Conduct access control assessments to identify current access management practices and challenges.
Year 2: Develop and implement access control policies and procedures that balance security requirements with business needs.
Year 3: Monitor access control effectiveness and adjust policies as needed to minimize friction while maintaining security.

Success Metrics:
Reduction in access-related security incidents, such as unauthorized access or data breaches.
Improvement in user satisfaction with access management processes, measured through surveys or feedback mechanisms.
Compliance with regulatory requirements related to access control and data protection.

6. Institute Resilient Detection and Response:

Goal Timeline:
Year 1: Enhance detection capabilities by deploying advanced monitoring tools and implementing threat intelligence solutions.
Year 2: Develop and document incident response procedures and conduct regular training and simulations for response teams.
Year 3: Continuously monitor and improve detection and response capabilities based on lessons learned from incidents and evolving threats.

Success Metrics:
Decrease in the time to detect and respond to security incidents, measured through key performance indicators (KPIs).
Improvement in incident response effectiveness, demonstrated by the containment and mitigation of incidents before they escalate.
Positive feedback from stakeholders on the organization's ability to detect and respond to security threats effectively.

Applicable Legal and Regulatory Requirements

Cybersecurity is a critical aspect of FIREARM's operations, and compliance with relevant legal and regulatory requirements is paramount to ensure the protection of sensitive information and the continuity of business operations. FIREARM acknowledges the importance of adhering to a comprehensive framework of laws, regulations, and industry standards that govern cybersecurity practices.

The Audit and Compliance team works closely with the Information Security Department, executive leadership, and external legal counsel to:

- Conduct regular assessments and audits to verify compliance with relevant regulations.
- Provide guidance and training to employees on cybersecurity laws, regulations, and best practices.
- Monitor changes in laws and regulations to update policies and procedures accordingly.
- Coordinate with external auditors and regulatory bodies for certifications and compliance validations.

This section outlines the key legal and regulatory requirements applicable to FIREARM's operations:

1. Government Security Regulations

Federal Protective Service (FPS) Regulations: These regulations govern security services provided to federal facilities and government officials. Compliance ensures adherence to FPS standards for physical security, access control, and threat response.

Federal Information Security Management Act (FISMA): FISMA regulations apply to security services involving federal government agencies. Compliance requires adherence to stringent cybersecurity controls, risk management practices, and security assessments.

Canadian Centre for Cyber Security (CCCS): Following CCCS guidelines for cybersecurity practices, particularly for government-related contracts and engagements.

2. Data Protection Regulations

General Data Protection Regulation (GDPR): Compliance with GDPR standards ensures the protection of personal data for clients, including executives and government officials.

Personal Information Protection and Electronic Documents Act (PIPEDA): Adherence to PIPEDA requirements for the secure handling of personal information, especially in client engagements.

3. Cybersecurity Laws and Regulations

Cybersecurity Information Sharing Act (CISA): Compliance with CISA provisions for sharing cybersecurity threat information, enhancing threat intelligence capabilities.

Data Breach Notification Laws: Adherence to laws mandating prompt notification of individuals and authorities in the event of a data breach, ensuring transparency and accountability.

4. Internation Standards and Frameworks

ISO/IEC 27001: Alignment with ISO/IEC 27001 standards for information security management systems, demonstrating commitment to best practices.

ISO/IEC 27002: Information security, cybersecurity privacy protection – information security controls. Becoming ISO certified, is the starting stage to secure our systems, data, network etc. This also helps in regaining government clearance.

ISO/IEC 27005: Information technology, security techniques – information security risk management.

ISO/IEC 31010:2019: Risk Management – Risk Assessment techniques

NIST Cybersecurity Framework: Following the NIST CSF for managing and reducing cybersecurity risks, enhancing overall security posture.

5. Privacy Regulations

Privacy Act: Compliance with Privacy Act provisions for the protection of personal information held by federal government departments and agencies, ensuring privacy rights are upheld.

Personal Information Protection Acts (PIPA): Adherence to provincial PIPA laws for the protection of personal information, safeguarding client and employee data.

Roles and Responsibilities

Board of Directors

Role: The Board of Directors holds ultimate responsibility for overseeing FireArm's risk management strategy and ensuring alignment with business objectives.

Responsibilities:

- Approve the overall risk management framework and policies.
- Review and provide guidance on risk appetite and tolerance levels.
- Receive regular reports on the organization's risk profile and mitigation efforts.
- Ensure compliance with legal, regulatory, and ethical standards related to risk management.

CEO

Role: The CEO provides strategic leadership and direction for the organization, including risk management initiatives.

Responsibilities:

- Champion the risk management culture and commitment throughout the organization.
- Approve major risk management decisions and initiatives.
- Engage with the Board of Directors on risk-related matters.
- Ensure that resources are allocated appropriately for risk management activities.

Chief Counsel (Legal)

Role: The Chief Counsel oversees legal matters and ensures that the organization operates within legal and regulatory frameworks.

Responsibilities:

- Provide legal guidance and advice on risk management policies and procedures.
- Review contracts, agreements, and compliance requirements related to risk management.
- Collaborate with the CISO and other stakeholders on legal implications of risk assessments and controls.

CISO

Role: The CISO is responsible for leading the Information Security Department and ensuring the organization's information assets are protected.

Responsibilities:

- Develop and maintain the risk management framework and policies.
- Oversee risk assessments, vulnerability assessments, and threat modeling.
- Implement controls and mitigation strategies to address identified risks.
- Report on the organization's risk posture to executive leadership and the Board of Directors.

Director of Cybersecurity

Role: The Director of Cybersecurity supports the CISO in managing the day-to-day operations of the Information Security Department.

Responsibilities:

- Assist in developing and implementing risk management processes and controls.
- Conduct risk assessments and support risk treatment efforts.
- Collaborate with IT teams to ensure security measures are integrated into systems and processes.
- Assist in preparing risk reports and updates for senior management.

CIO

Role: The CIO oversees the organization's IT strategy and ensures that IT systems support business objectives.

Responsibilities:

- Align IT initiatives with the organization's risk management strategy.
- Ensure that IT systems are designed, implemented, and operated securely.
- Collaborate with the CISO and cybersecurity team on risk assessments and mitigation efforts.
- Provide input on IT-related risks and vulnerabilities to the risk management process.

Audit & Compliance Officer

Role: The Audit & Compliance Officer is responsible for ensuring that the organization adheres to internal policies and external regulations.

Responsibilities:

- Conduct internal audits to assess compliance with risk management policies.
- Identify gaps in controls and recommend corrective actions.
- Monitor regulatory changes and update risk management practices accordingly.
- Collaborate with the CISO and risk management team on audit findings and remediation efforts.

Chief Risk Officer

Role: The Chief Risk Officer leads the organization's overall risk management efforts and ensures a holistic approach to risk mitigation.

Responsibilities:

- Develop and maintain the enterprise risk management framework.
- Coordinate risk assessments across departments and business units.
- Monitor risk metrics and trends to inform strategic decision-making.
- Provide regular risk reports to executive leadership and the Board of Directors.

IAM Manager

Role: The IAM Manager is responsible for managing user access to IT systems and ensuring appropriate access controls.

Responsibilities:

- Implement and maintain identity and access management policies and procedures.
- Conduct access reviews and ensure compliance with least privilege principles.
- Collaborate with the CISO and IT teams on access-related risks and controls.
- Provide support for user authentication, authorization, and provisioning processes.

IT Operations

Role: The IT Operations team is responsible for the day-to-day management and maintenance of IT systems and infrastructure.

Responsibilities:

- Implement and maintain security controls and configurations on IT systems.
- Monitor systems for security incidents and vulnerabilities.
- Collaborate with the cybersecurity team on risk mitigation efforts.
- Follow established procedures for incident response and recovery.

Security Incident Response/ Security Ops Manager

Role: The Security Incident Response/ Security Operations Manager leads the organization's response to security incidents and manages security operations.

Responsibilities:

- Develop and maintain incident response plans and procedures.
- Coordinate responses to security incidents, including containment and recovery.
- Monitor security events and alerts to detect potential threats.
- Conduct post-incident reviews and implement lessons learned for continuous improvement.

Asset Owner

Roles: The Asset Owner is accountable for the confidentiality, integrity, and availability of information assets created and used to carry out a department’s business operational functions.

Responsibilities:

- Setting and determining the budget associated with an Information System and the informational assets processed through this system.
- Approving risk treatment plans and providing oversight on any remediation associated with information systems and assets.
- Authorizing a designate (Asset Delegate) to act on his/her behalf as needed.

Asset Delegate

Roles: The Asset Delegate is accountable for managing the risk(s) to the asset.

Responsibilities:

- Classifying the Information Asset(s) based on their sensitivity and importance to the organization.
- Determining the regulatory requirements applicable to the Information Asset(s).
- Providing business-specific requirements, including security requirements, to ensure proper protection of the assets.
- Ensuring that an Information Security risk assessment is completed for Information Assets within his/her departments where applicable.
- Determining, authorizing, and/or making recommendations for risk treatment plans for their Information Asset(s).
- Performing regular reviews of the progress of risk treatment plans and assessing the remaining residual risk for assigned Information Asset(s).

Human Resources

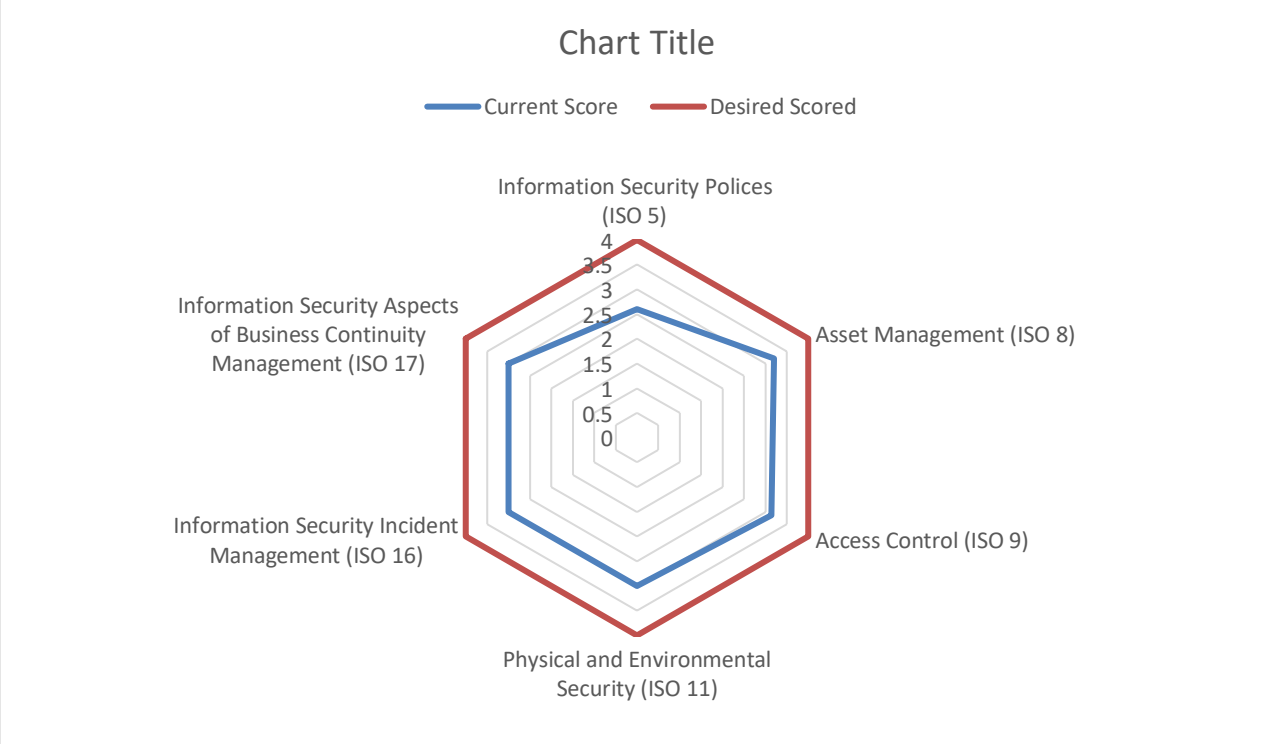
Role: The Human Resources department plays a critical role in supporting risk management efforts related to personnel and workforce policies.

Responsibilities:

- Ensure that employees receive security awareness training and adhere to security policies.
- Collaborate with the CISO and cybersecurity team on employee onboarding and offboarding processes.
- Support investigations into security incidents involving employees.
- Provide guidance on employee disciplinary actions related to security violations.

Results of a Security Controls Gap Assessment

Summary Results Overview



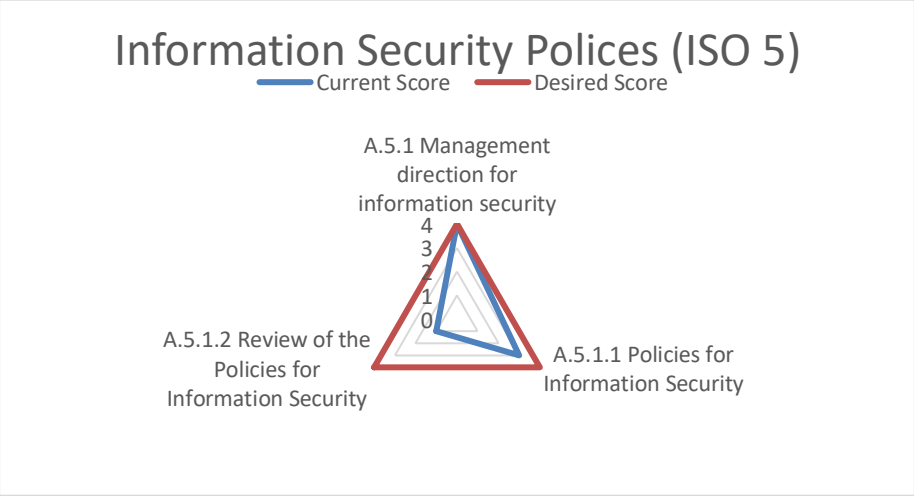
Information Security Polices (ISO 5)

The Controls: The primary control in ISO 5 is:

5.1 Management Direction for Information Security

Objective: To determine whether the organization has an information security policy that has been formally approved by upper management.
This aspect of cybersecurity governance entails the establishment, communication, and enforcement of policies that guide the organization's approach to safeguarding sensitive information assets.

Assessment Result: FireArm's management direction information security is in *below average* condition with none of the sub-domains in complete compliance, amounting to two (2) of the sub-domains requiring corrective action.



Security Controls that are in a state of nonconformity and require corrective action:

1. 5.1.2 Review of the Policies for Information Security at Maturity Level: 1
2. 5.1.1 Policies for Information Security at Maturity Level: 3

Recommendations:

5.1.2 Review of the Policies for Information Security at Maturity Level: 1

Recommendations and Corrective Actions:

- Define specific intervals for formal reviews and audits of the information security policy, considering factors such as business cycles, regulatory changes, and emerging threats. Upon review and audit, if need arises schedule policy updation.

5.1.1 Policies for Information Security at Maturity Level: 3

Recommendations and Corrective Actions:

- Implement a multi-channel approach to communicate the security policy, including email notifications, internal newsletters, and posters in common areas.
- Ensure that the security policy is easily accessible on the company's intranet or internal portal. Consider creating a dedicated section with FAQs, examples, and case studies for better understanding.
- Implement a process where employees must acknowledge receipt and understanding of the security policy. This could be done during onboarding and periodically thereafter.

Asset Management (ISO 8)

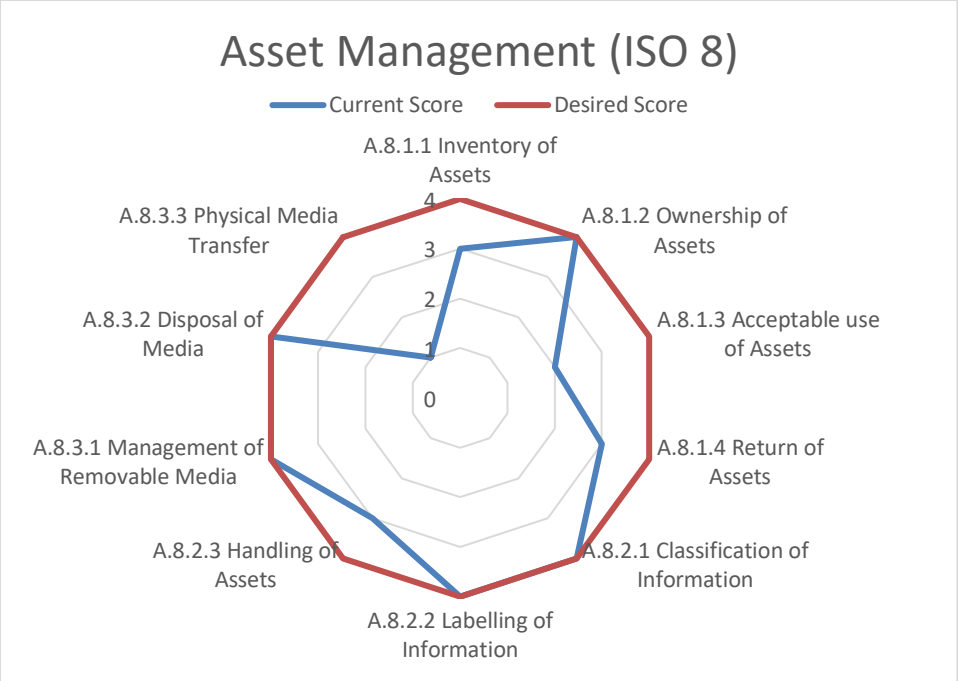
The Controls: The primary controls in ISO 8 are:

8.1 Responsibility for assets
Objective: To identify organizational assets and define appropriate protection responsibilities.

8.2 Information classification
Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to FireArm.

8.3 Media handling
Objective: To prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.

Assessment Result: FireArm's asset management is in *below average* condition with only five (5) of the ten (10) sub-domains in compliance and five (5) of the sub-domains that have nonconformities and require corrective action.



Security Controls that are in a state of nonconformity and require corrective action:

1. 8.3.3 Physical Media Transfer at Maturity Level: 1
2. 8.1.3 Acceptable use of Assets at Maturity Level: 2
3. 8.1.4 Return of Assets at Maturity Level: 3
4. 8.2.3 Handling of assets at Maturity Level: 3

Recommendations:

8.3.3 Physical media Transfer at Maturity Level: 1

Recommendations and Corrective Actions:
Any media containing information should be protected against unauthorized access.

8.1.3 Acceptable use of Assets at Maturity Level: 2

Recommendations and Corrective Actions:
"Acceptable use Policy" should be made available to employees, customers and the security guards.

8.1.4 Return of Assets at Maturity Level: 3

Recommendations and Corrective Actions:
Document that manages the list of return assets should be verified and reviewed frequently. In case of non-return of organizational asset unless agreed upon an agreement, security incident should be created immediately.

8.2.3 Handling of assets at Maturity Level: 3
Recommendations and Corrective Actions:
Access restriction to the information about customers must be implemented.

Acess Control (ISO 9)

The Controls: The primary controls in ISO 9 are:

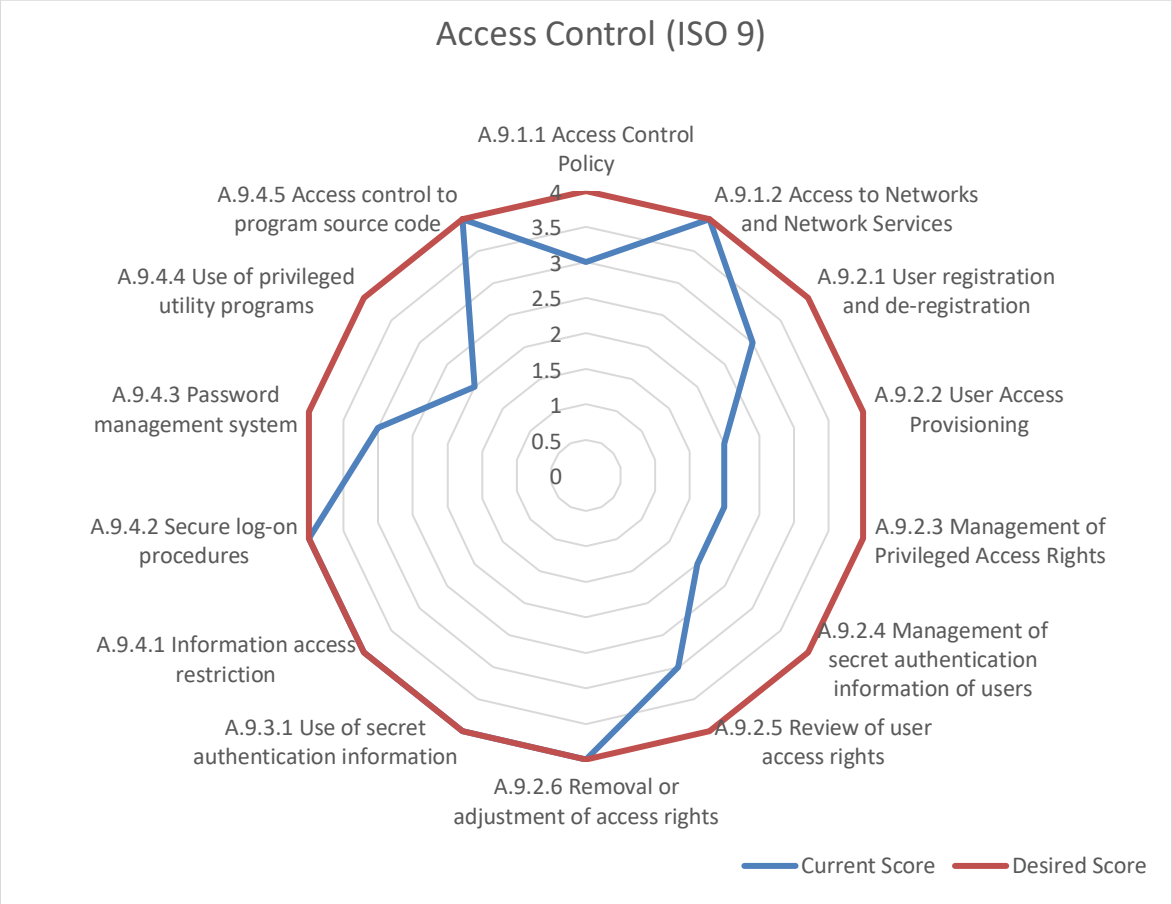
16.1 Business requirements of access control
Objective: To limit access to information and information processing facilities.

16.2 User access management
Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

16.3 User responsibilities
Objective: To make users accountable for safeguarding their authentication information.

16.4 System and application access control
Objective: To prevent unauthorized access to systems and applications.

Assessment Result: FireArm's access control is in *below average* condition with none of the sub-domains in compliance amounting to fourteen (14) of the sub-domains with nonconformities and that require corrective action.



Security Controls that are in a state of nonconformity and require corrective action:

1. 9.2.2 User Access Provisioning at Maturity Level: 2
2. 9.2.3 Management of Privileged Access Rights at Maturity Level: 2
3. 9.2.4 Management of secret authentication information at Maturity Level: 2
4. 9.4.4 Use of privileged utility programs at Maturity Level: 2
5. 9.2.5 Review of user access rights at Maturity Level: 3

Recommendations:

9.2.2 User Access Provisioning at Maturity Level: 2

Recommendations and Corrective Actions:
Process must be implemented to assign or revoke access rights for all users types to services that FIREARM provides.

9.2.3 Management of Privileged Access Rights at Maturity Level: 2

Recommendations and Corrective Actions:
A process and record of all privileges allocated should be maintained (alongside the information asset inventory) and the competence of users granted the rights must be reviewed regularly to align with their duties.

9.2.4 Management of secret authentication information at Maturity Level: 2
Recommendations and Corrective Actions:
Any default secret authentication information provided as part of a new system use should be changed as soon as possible

9.4.4 Use of privileged utility programs at Maturity Level: 2
Recommendations and Corrective Actions:
Use of utility programmes should be logged and monitored/reviewed periodically to satisfy auditor requests.

9.2.5 Review of user access rights at Maturity Level: 3
Recommendations and Corrective Actions:
Amend the procedures frequently and review those periodically for the access rights, roles with privileged access.

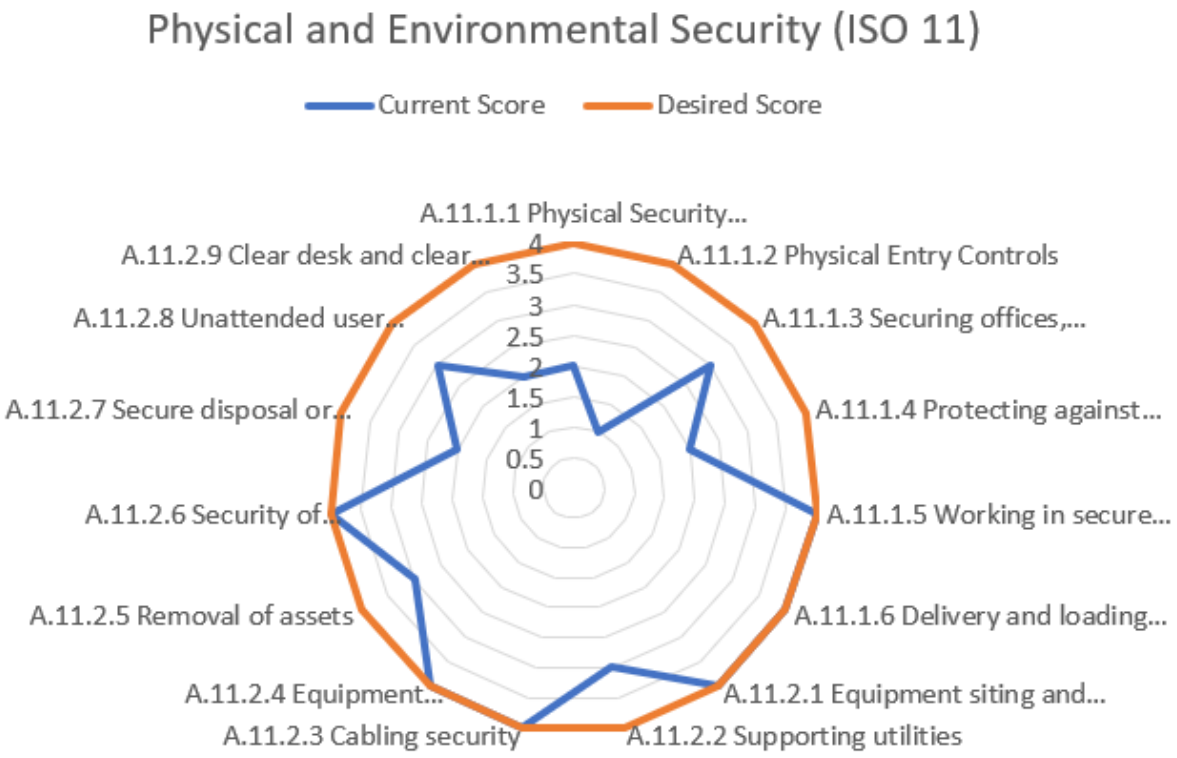
Physical and Environmental Security (ISO 11)

The Controls: The primary controls in ISO 11 are:

16.5 Secure areas
Objective: To prevent unauthorized physical access, damage and interference to FIREARM's information and information processing facilities.

16.6 Equipment
Objective: To prevent loss, damage, theft or compromise of assets and interruption to FIREARMS's operations.

Assessment Result: FireArm's physical and environmental security is in *average* condition with ten (10) of the fifteen (15) sub-domains in compliance and five (5) sub-domains with nonconformities and that require corrective action.



Security Controls that are in a state of nonconformity and require corrective action:

1. 11.1.2 Physical Entry Controls at Maturity Level: 1
2. 11.1.1 Physical Security Perimeter at Maturity Level: 2
3. 11.1.4 Protecting against external and environmental threats at Maturity Level: 2
4. 11.1.3 Security offices, rooms, and facilities at Maturity Level: 3
5. 11.2.5 Removal of assets at Maturity Level: 3

Recommendations:

11.1.2 Physical Entry Controls at Maturity Level: 1

Recommendations and Corrective Actions:
Along with the existing controls, additional controls like Iris scanner, fingerprint sensors should be placed.

11.1.1 Physical Security Perimeter at Maturity Level: 2

Recommendations and Corrective Actions:
FIREARM must establish much more secure areas where the information and assets are placed.

11.1.4 Protecting against external and environmental threats at Maturity Level: 2

Recommendations and Corrective Actions:
Get advice from disaster management experts on ways to avoid damage by fire, or natural disasters.

11.1.3 Security offices, rooms, and facilities at Maturity Level: 3

Recommendations and Corrective Actions:
Visitors must be escorted to some secure areas.

11.2.5 Removal of assets at Maturity Level: 3

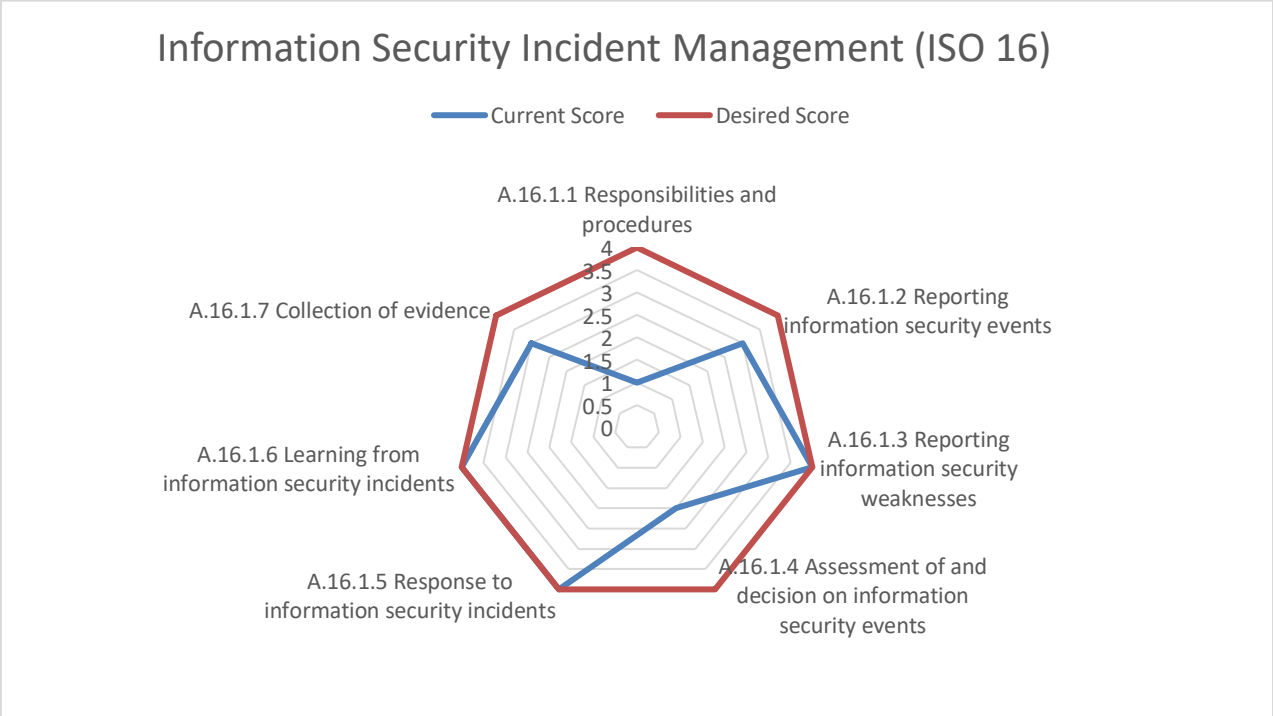
Recommendations and Corrective Actions:
Equipment that the security guard's taken off-site must be implemented with basic check in/check out process.

Information Security Incident Management (ISO 16)

The Controls: The primary control in ISO 16 is:

16.1 Management of Information Security incidents and improvements.
Objective: To ensure a consistent and effective approach to the identification, response, and management of information security incidents within the organization. This control aims to establish procedures and processes that enable prompt and efficient actions when security incidents occur, with the overarching goal of minimizing the impact on the organization's operations, data, and reputation.

Assessment Result: FireArm's information security incident management is in *average* condition with six (6) of the eight (8) sub-domains in compliance and two (2) sub-domains with nonconformities and that require corrective action.



Security Controls that are in a state of nonconformity and require corrective action:

1. 16.1.1 Responsibilities and procedures at Maturity Level: 1
2. 16.1.4 Assessment of and decision on information security events at Maturity Level: 2

Recommendations:

16.1.1 Responsibilities and procedures at Maturity Level: 1

Recommendations and Corrective Actions:

- FireArm should develop detailed incident response procedures that outline step-by-step actions to be taken when a security incident occurs.
- Clearly define roles and responsibilities for incident response team members to ensure a coordinated and efficient response.
- Implement standardized procedures for reporting security events and incidents throughout the organization.
- Ensure that incident-handling procedures cover the entire incident life cycle, from detection to resolution.
- Align incident response procedures with business continuity and disaster recovery plans for a holistic approach to resilience.

16.1.4 Assessment of and decision on information security events at Maturity Level: 2

Recommendations and Corrective Actions:

- Define a set of standardized criteria for assessing the severity and impact of security events.
- Ensure these criteria align with industry best practices and regulatory requirements.

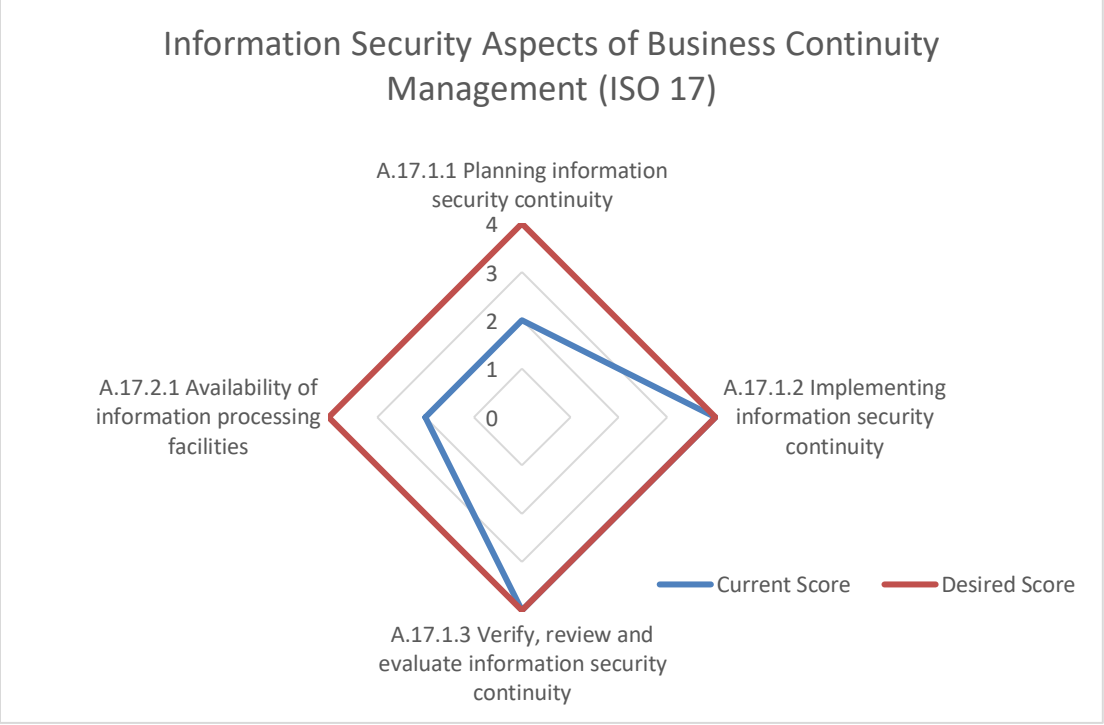
Information Security Aspects of Business Continuity Management (ISO 17)

The Controls: The primary control in ISO 17 is:

17.1 Information security continuity

Objective: To ensure the organization has established robust controls and plans to maintain the continuity of information security operations. This includes having a well-documented business continuity plan specifically tailored for information technology (IT), based on a thorough business impact analysis, regularly tested, and approved by management.

Assessment Result: FireArm's information security aspects of business continuity management is in *average* condition with two (2) of the four (4) sub-domains in compliance and two (2) sub-domains with nonconformities and that require corrective action.



Security Controls that are in a state of nonconformity and require corrective action:

1. 17.1.1 Planning information security continuity at Maturity Level: 2
2. 17.2.1 Availability of information processing facilities at Maturity Level: 2

Recommendations:

17.1.1 Planning information security continuity at Maturity Level: 2

Recommendations and Corrective Actions:

- Create a detailed IT disaster recovery plan that outlines procedures, roles, responsibilities, and steps to be taken in the event of a disaster or disruption. Include sections on data backup and recovery, system restoration, communication protocols, alternate work arrangements, and post-incident analysis.
- Conduct regular testing of the IT disaster recovery plan through tabletop exercises or simulated drills.
- Share the IT disaster recovery plan with business partners, stakeholders, and trustees for validation and feedback.

17.2.1 Availability of information processing facilities at Maturity Level: 2

Recommendations and Corrective Actions:

- Invest in redundant hardware components such as servers, storage devices, and network equipment. This includes having redundant power supplies, disk arrays, and network switches.
- Use technologies like RAID (Redundant Array of Independent Disks) for data storage to ensure data availability even if a disk fails.
- Have redundant internet connections from different service providers to ensure continuous connectivity.
- Implement robust monitoring tools to continuously monitor the health and performance of redundant systems.

Results of a Risk Assessment

Classification Scheme

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.

Sample Asset Inventory

	Asset Inventory - Step 1					
ID	Name of Asset	Description of Asset	Type of Asset	Asset Owner (Accountable) Name / Role / Dept.	Classification	Location of Asset
1	Customer data	Sensitive personal and transactional information collected from clients (contact details, purchase history, Birthdate, Address)	Information	IT	Confidential	AWS
2	Financial statements	Summarized records presenting the financial position, performance, and cash flows of a company.	Information	Finance	Confidential	Financial management software
3	Employee data	Confidential information comprising personal details, employment history, and performance metrics of company staff.	Information	IT	Confidential	HR information system
4	Access logs	Detailed records documenting user interactions, providing insights into system access and activity for security analysis and auditing purposes.	Information	IT	Internal	HR information system
5	Non-disclosure agreements	Legal contracts outlining confidentiality obligations between parties regarding sensitive information.	Information	Legal	Internal	Document management system
6	Contractual Agreements	Legal agreements outlining terms, conditions, and obligations between parties.	Information	Legal	Internal	Document management system
7	Strategic Plans	Comprehensive blueprints outlining long-term objectives and initiatives critical for organizational success.	Information	Managing director	Internal	Document management system
8	Encryption keys	Digital codes used to encrypt and decrypt sensitive data, ensuring secure communication and protection against unauthorized access.	Information	IT	Restricted	Key management system
9	Annual reports	Comprehensive summaries of a company's financial performance, including income statements, balance sheets, and cash flow statements, typically released on an annual basis.	Information	Managing director	Public	Company website
10	Company polices	Outlined rules, guidelines, and procedures governing employee conduct, organizational operations, and compliance standards.	Information	Managing director	Public	HR system
13	Credentials	User authentication information, including usernames, passwords, access tokens, and digital certificates, used to verify identity and grant access to systems, applications, and data.	Information	IT	Restricted	Active Directory

Security Impact Analysis

		Security Impact Analysis - Step 2						
ID	Name of Asset	Confidentiality	Integrity	Availability	Regulatory	Reputational	Financial	Impact Rating
1	Customer data	Very High	High	High	High	High	Medium	High
2	Financial statements	Very High	High	High	High	High	High	High
3	Employee data	Very High	High	High	High	High	Medium	High
4	Access logs	Medium	High	High	Low	Medium	Low	Medium
5	Non-disclosure agreements	High	Medium	Medium	Medium	Medium	Medium	Medium
6	Contractual Agreements	High	High	High	Medium	Medium	Medium	High
7	Strategic Plans	High	High	High	Medium	Medium	Medium	High
8	Encryption keys	Very High	Very High	High	High	High	High	Very High
9	Annual reports	Low	High	Medium	Medium	High	Low	Medium
10	Company polices	Low	High	Medium	Medium	Medium	Low	Medium
13	Credentials	High	High	High	High	High	High	High

Threat Exposure (Risk) Ratings

	Step 3	Step 3a	Step 4	
Name of Asset	Threat Description	Threat Likelihood	Threat Exposure Rating	Threat Exposure Rating Number
Customer data	Information leakage	Almost certain	High	7
Financial statements	Information leakage	Almost certain	High	7
Employee data	Information leakage	Almost certain	High	7
Access logs	Unauthorized changes of records	Likely	Medium	5
Non-disclosure agreements	Unauthorized changes of records	Likely	Medium	5
Contractual Agreements	Unauthorized changes of records	Likely	High	6
Strategic Plans	Unauthorized changes of records	Likely	High	6
Encryption keys	Theft	Likely	High	7
Annual reports	Unauthorized changes of records	Likely	Medium	5
Company polices	Information leakage	Almost certain	High	6
Credentials	Disclosure of passwords or credentilas	Likely	High	6

Risk Management Strategy

Vulnerability Identification

	Step 5	
Name of Asset	**Vulnerability Description**	**Vulnerability Severity**
Customer data	Subject to phishing	High
Financial statements	Single copy	High
Employee data	Subject to phishing	High
Access logs	Lack of access control policy	High
Non-disclosure agreements	Lack of internal documentation	High
Contractual Agreements	Lack of internal documentation	High
Strategic Plans	Lack of internal documentation	High
Encryption keys	Inadequate protection of cryptographic keys	Medium
Annual reports	Lack of internal documentation	High
Company polices	Lack of internal documentation	High
Credentials	Subject to phishing	High

Evaluation of Existing Safeguards and Residual Risk Ratings

	Step 6			Step 7	
Name of Asset	**Primary Safeguard**	**Primary Safegaurd ID**	**Primary Safeguard Rating**	**Residual Risk Rating**	**Residual Risk Number**
Customer data	7.2.2 Information security awareness, education and training	ISO-013	Low	High	4
Financial statements	5.1.1 Information security policy document	ISO-001	Medium	High	4
Employee data	7.2.2 Information security awareness, education and training	ISO-013	Low	High	4
Access logs	9.2.2 User access provisioning	ISO-029	Medium	Medium	3
Non-disclosure agreements	8.2.3 Information handling	ISO-022	Low	High	4
Contractual Agreements	8.2.3 Information handling	ISO-022	Low	High	4
Strategic Plans	6.1.1 Management commitment	ISO-003	Medium	High	4
Encryption keys	5.1.1 Information security policy document	ISO-001	Medium	Medium	3
Annual reports	8.2.3 Information handling	ISO-022	Medium	Medium	3
Company polices	8.2.3 Information handling	ISO-022	Medium	High	4
Credentials	7.2.2 Information security awareness, education and training	ISO-013	High	Medium	3

Maintaining the Risk Register

IT Risk Register											
ID	**Name of Asset**	**Risk Decision**	**Risk Owner**	**Mitigation Strategy**	**Mitigation Owner**	**Risk Analyst**	**Start Date**	**Due Date**	**Mitigation Completion Date**	**Status**	**Initial Date of Assessment**
#	*From Risk Assessment*	*Risk treatment options for Asset Owner*	*Who is accountable for the risk?*	*Risk treatment plan*	*Who is accountable for the risk treatment?*	*Who is responsible for the risk treatment?*	*Date risk treatment commenced*	*Projected date of risk treatment completion*	*Actual date of risk treatment completion*	*Status of risk treatment*	*From Risk Assessment*
1	Customer Database	REDUCE	VP Operations		Director Operations	John Phive	4-6-2024	8-6-2024		In progress	3-6-2024
2	FireArm Mobile Application	REDUCE	VP Development		Director Development	Adam Penner	4-7-2024	8-7-2024		Pen test	3-7-2024
3	Employee Training and Skills Database	REDUCE	VP Database		Director Database	Joseph Ruderford	4-8-2024	8-8-2024		In review	3-8-2024
4	Employee Workstation (Asset No. 0086428)	REDUCE	VP IT		Director IT	Christian Bale	4-9-2024	8-9-2024		Hold pending additional information	3-9-2024
5	Employee Phone (Asset No. 0086427)	REDUCE	VP IT		Director IT	Billy Boden	4-10-2024	8-10-2024		In review	3-10-2024
6	Employee Laptop (Asset No. 0086429)	REDUCE	VP IT		Director IT	Chris Gayle	4-11-2024	8-11-2024		In progress	3-11-2024

Vendor Registry

Business Name	Website	Description
Microsoft O365	microsoft.com	Office 365 & associated services
Salesforce	https://www.salesforce.com/	Sales Management
Online Business Systems	www.OBSglobal.com	Security Consulting with access to network and sensitive information
ADP Workforce Now	https://www.adp.com/logins/adp-workforce-now.aspx	Human resource management service
Commvault (Metallic)	https://www.commvault.com/complete-data-protection/backup-a	O365 Backup Service
Royal Bank of Canada	https://www.rbc.com/canada.html	Banking
AgileBlue	www.agileblue.com	Managed security monitoring
Security scorecard	www.securityscorecard.com	Vendor Security Management
ASSA ABLOY	www.assaabloy.com	Lock and Security solutions

Vendor Risk Management

Business Name	Access (Describe)	Assets (Desctribe)	Asset Classification	Category	RiskRecon Report	ISO27 K	SOC 2 Cer	Policy & Stand	Questionnaire Ratin	Contract Risk	NDA Signed?	Risk Rating
Microsoft O365	Admin / User	Store, Process	Restricted	Tier 1	C 5.8/10	Y	Y	Y	NA	LOW	N	Moderate
Salesforce	No	Store, Process	Confidental	Tier 1	B 8.0/10	Y	Y	Y	NA	LOW	N	Low
Online Business Systems	Admin / User	Store, Process	Restricted	Tier 1	A 9.8/10	N	N	Y	9.5/10	LOW	Y	Low
ADP Workforce Now	No	Store, Process	Restricted	Tier 2	B 8.2/10	Y	Y	Y	NA	Medium	N	Low
Commvault (Metallic)	User	Store, Process	Restricted	Tier 2	A 8.6/10	N	N	Y	7.3/10	High	Y	High
Royal Bank of Canada	No	Store, Process	Restricted	Tier 2	B 8.0/10	Y	Y	Y	NA	LOW	N	Low
AgileBlue	Admin / User	Store, Process	Restricted	Tier 2	B 7.6/10	N	N	Y	8.5/10	Medium	N	Moderate
Security scorecard	No	Store, Process	Public	Tier 2	B 7.8/10	N	N	Y	8.2/10	High	N	High
ASSA ABLOY	Admin	Store, Process	Restricted	Tier 1	C 5.7/10	N	N	Y	1.44/5	High	Y	High

Concluding Remarks

If the recommendations resulting from the aforementioned assessments are adopted in accordance with industry best practices, our security posture will significantly improve. This progression sets us on a trajectory towards ISO certification.

Below are the anticipated criteria for implementing the aforementioned recommendations.

Expected Time to Complete	1-3 years
Expected Cost	$ 2,98,000
Expected Control Posture	2.99 -> 3.9

Document History

Document Information

Document Name	Cybersecurity Business Plan
Electronic File Name	Cybersecurity Business Plan.pdf
File Location	Dropbox

Revision History

Version	Date	Author	Description of Revision
0.1	April 2024	Sarah Syeda	Initial Draft

Author:
Sarah Syeda
Director of Cybersecurity
FireArm

Email: sarah.syeda@ucalgary.ca

Contact: +1 368-299-8592

Reporting to:
Mike Primeau, CISO
FireArm

References

[1] Rational Cybersecurity for Business - a security leaders guide to business alignment by Dan Blum

[2] Asset Inventory & Risk Assessment TOOL

[3] HACME ISO 27002 Assessment REPORT v0.03 DRAFT

[4] eBook_The_Anatomy_of_a_Third_Party_Data-Breach

[5] detailed-report-Securitas-AB-485791274-2024-3-5_23-37-48

[6] ISO 27000:2014 – Information Technology – Security Techniques – Information security management systems – Overview and vocabulary

[7] ISO 27002:2022 Information Security, cybersecurity and privacy protection – Information security controls

[8] ISO 27005:2011 – Information Technology – Security Techniques – Information security risk management

[9] ISO 31000:2018 – Risk Management – Principles and guidelines

[10] ISO 31010:2019 – Risk Management Risk Assessment Techniques

List of Attached Appendices

APPENDIX A: GLOSSARY

Confidentiality: A set of rules, or a promise usually executed through confidentiality agreements that limits the access or places restrictions on certain types of information.

Integrity: Integrity is the practice of being honest and showing a consistent and uncompromising adherence to strong moral and ethical principles and values

Availability: For any information system to serve its purpose, the information must be available when it is needed.

Asset: An asset is any data, device, or other component of the environment that supports information-related activities.

Threat: Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Risk: the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of occurrence of an event and its consequence.

Vulnerability: Vulnerabilities are flaws in a computer system that weaken the overall security of the device/system.

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authorization: the function of specifying access rights/privileges to resources, which is related to general information security and computer security, and to access control in particular

Accountability: The traceability of actions performed on a system to a specific system entity System: Any electronic device that is managed and owned by FIREARM

Gap Assessment: identifies gaps between the optimized allocation and integration of the inputs (resources), and the current allocation-level

Risk assessment: A risk assessment is the combined effort of: identifying and analyzing potential (future) events that may negatively impact individuals, assets, and/or the environment

Vulnerability assessment: A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system

APPENDIX B: Success Plan Worksheet