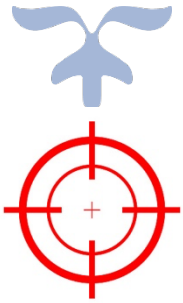
CYBERSECURITY BUSINESS PLAN

FIREARM



Author: Prajwal Thippeswamy
Reporting to: James Clear (CISO, FireArm)

Table of Contents

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
0.01	December 2022	Prajwal Thippeswamy	Initial draft

Author:
Prajwal Thippeswamy
Director of Cybersecurity,
FireArm
Email: prajwal.thippeswamy@firearm.ca
Contact number: +1234567890

Reporting to:
James Clear, CISO
FireArm

Executive Summary

FireArm is an industry leader in providing private security services for executives, government officials and site surveillance services. FIREARM Security Services was founded in 2010 with passion of delivering world-class security solutions to Alberta, Edmonton, Calgary, and surrounding arias. With more than 6 years of experience, we have been providing quality and consistent security services across a portfolio of businesses.

We demonstrate our commitment to making people feel safe by partnering with individuals and companies who share our vision, and by providing security services and implementing security strategies specific to our client needs.

Vision

To be the best at making people feel safe by inspiring our staff to "believe they can make a difference" in everything they do.

Mission

To be the best at making people feel safe by inspiring our staff to "believe they can make a difference" in everything they do.

Brief Intro about the data breach

The recent data breach (3 April 2022) that FireArm encountered has made government to revoke the clearance. Not only this incident affected our organization's reputation but also, we incurred a 10 million USD loss. Therefore, our team, performed security analysis and found that this breach would have been prevented if we had formal security program and be ISO 27002 compliant initially, then get ISO 31000 certified.

Our analysis also projects that if the recommendations, that are provided at the end of Risk Management process, could increase the security controls posture 49% (current) to 75% (expected).

Background

FireArm suffered a data breach on April 3, 2022. The customer information was leaked including government official's personal identifiable information. Corporate espionage and insider threat are being considered. After investigation, the root cause of this incident was a malware executed on a USB key using a contractor's credentials to gain access to FireArm's network and sensitive data. FireArm's leadership group is concerned about the company's reputation and the risk of losing their government clearance.

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.

FireArm has had their government clearance revoked until their management team has demonstrated a remediation roadmap in their information security program.

The Process

Considering the security auditors findings, lack of formal cybersecurity program is the reason for the cybersecurity data breach that we encountered on April 3, 2022.

The Pareto Principle states that approximately 80% of consequences come from 20% of the causes. This applies to enterprise cybersecurity: the unsung 20% of our tooling that brings over 80% of the value.

As a method to construct formal cybersecurity program, following priorities need to be assessed, improved, monitored, and created if absent.
Priorities:

1. Risk Management
2. Control Baseline
3. Security Culture,
4. IT rationalization
5. Access control
6. Cyber-resilience

Assessing Current Security Posture

1. Gap Assessment: Performed Control Gap Assessment using **ISO/IEC 27002**
2. Threat and Risk Assessment (TRA): Performed Risk Assessment using **ISO/IEC 27005**

Recommendations to increase Future Security Posture
Risk Treatment: From the outcomes of Gap Assessment and Threat and Risk Assessment (TRA), risk treatment has been formulated. Some of the critical processes that disrupt the business in risk treatment stage are pending, which will be handled once the funds are approved and released.

Scope of Work

Scope and Applicability

FIREARM Information Security Department defines Information Security as “the processes and mechanisms by which FIREARM’s digital information assets, IT infrastructure and related services are protected from unintended or unauthorized access, change or destruction”.

FIREARM’s Information Security Department is accountable for the Gap Assessment, Risk Management program and related processes.

This document deals with the process and procedures used within the Risk Management and will provide guidance to FIREARM Asset Owners and Stakeholders on how to identify, analyze, document, and manage Information Security risks to a tolerable level to minimize adverse effects to FIREARM’s Asset. The Risk Management is applicable to all FIREARM Information and IT related Assets.

Out of Scope

This program and related processes do not apply to identifying or reporting FIREARM general risks that are not specific to IT Services. Third party risk assessment (TRA) is also out of scope.

Applicable legal and regulatory requirements

This program provides the minimum requirements for conducting a risk assessment. FIREARM. Information Security does not mandate a specific industry risk framework or methodology; however, it has adopted a “fit for purpose” hybrid approach to ensuring the tasks performed are in line with recognized industry methodologies.

Conducting extensive research and suggestions from the industry leaders, becoming ISO certified, is the starting stage to secure our systems, data, network etc. This also, helps in regaining the government clearance.

Some of the Industry Standard Information Security Risk frameworks and methodologies referenced include:

- ISO 31010:2019, Risk Management – Risk assessment techniques.
- ISO 31000:2018, Risk Management – Guidelines
- ISO 27005; Information technology – Security techniques – Information security risk management.
- ISO/IEC 27002:2022, Information security, cybersecurity privacy protection – Information security controls

ISO/IEC 27001:2022, Information security, cybersecurity privacy protection – Information security management systems - Requirements

Roles and Responsibilities

FIREARM's Risk Management is designed to provide a means for Information Security Department to execute and meet the delivery of a comprehensive risk management program to ensure that IT risks are consistently identified, assessed, evaluated, controlled/mitigated, treated, reviewed, and reported.

FIREARM has defined roles and responsibilities at various levels to ensure this process is followed in a consistent manner.

- **Board of Directors**: Will be informed of the results of IT risk assessments that have resulted in High or Very High Residual Risk.

- **FIREARM Corporate Risk Management**: Will be informed of the results of IT risk assessments that have resulted in Medium, High or Very High Residual Risk. As stewards or the Enterprise Risk Management Registry, all IT risk assessments that have resulted in Medium, High or Very High Residual Risk will be updated in the Enterprise Risk Management Registry.

- **Chief Information Security Officer (CISO)**: Has overall accountability for Information Security Risk Management (Risk Management) program but has delegated the development and operational responsibilities to the Director, IT Infrastructure & Security. This role provides support, oversight, direction, and final approval of the Risk Management program. Responsible to enable the Information Security Risk Management program with the appropriate level of authority, time, training, resources, and skills.

- Director, Information Security: Has accountability and responsibility for I.T. Security and and for the process owner for the Information Security Risk Management program. This role is accountable for:

    - Ensuring that risk associated with IT Assets are fully assessed and treated.
    - Ensuring that operational risk associated with changes to the HACME network environment is well managed as it pertains to the Risk Assessment Criteria.
    - Ensuring that Information Security risks are fully considered in the development of long-term strategies and plans.
    - Reviewing and managing Information Security Risk governance issues and recommended strategies to respond to risk where appropriate.
    - Participating in the review and approval process regarding IT Risk Assessment Report recommendations, ITS Risk Management decision(s) and/or risk treatment plans.
    - The ongoing development, implementation, maintenance, operational service and continuous improvement of the Risk Management methodologies and associated standards.

  - Ensuring consistent application of the ITS Risk Management program throughout FIREARM where applicable.
  - Providing training, guidance, and support to ensure risk standards, measures, and methodologies are consistently applied.
  - Supporting the use of risk management processes and tools.

- **Asset Owner**: This role is ultimately accountable for the confidentiality, integrity, availability, classification, use and final disposition of information assets created and used to carry out a department's business operational functions.
  - This role typically sets and determine budget associated with an Information System and the Informational Asset processed through this system.
  - This role approves risk treatment plans and provides oversight on any remediation associated with information systems and assets.
  - As all information requires an Asset Owner, the Asset Owner may authorize a designate (Asset Delegate) to act on his/her behalf.

- **Asset Delegate**: This role is accountable for managing the risk(s) to the asset. The Asset Delegate may delegate a portion of their responsibilities to an Asset Custodian; however, the Asset Delegate remains accountable for the following activities:
  - Classification of the Information Asset(s);
  - Determining regulatory requirements of the Information Asset(s);
  - Providing business specific requirements including security requirements.
  - Ensuring an Information Security risk assessment is completed for Information Assets within his/her departments where applicable;
  - Determine and authorize and/or risk treatment plans and/or recommendations for their Information Asset(s); and
  - Perform regular review of the progress of risk treatment plan(s) and remaining residual risk for assigned Information Asset(s).

- **Asset Custodian**: This role is assigned by the Information Asset Owner or by the Director, IT Infrastructure & Security. This role may also be filled by a Service Provider. Owner.
  - The role could be filled by an individual or committee accountable for the Information Management Practice within their area of responsibilities. This role is directly accountable back to the Information Owner for a specific dataset.
  - This role could be a FIREARM department or external organization(s) whose responsibilities include:
    - architecting,
    - securing and
    - operating those technology assets and associated process on behalf of the Asset Owner.

- Project Managers & Business Analysts: As responsible for ensuring that IT Risk Assessments are factored into to the initiating & planning phases of all projects that include information assets.

The Role of the FIREARM Gap & Risk Assessor

The Information Security Gap & Risk assessor's role is to effectively communicate and provide advisory services to the Asset Owners, Stakeholders and/or project team. During the process if any high/very high risks are identified, the assessor will communicate and consult with the stakeholders to discuss Risk Treatment during solution development and prior to finalizing the Risk Assessment Report. This action provides an opportunity for the Asset Owner and Stakeholders and./or project team to address identified risk(s) prior to implementing a solution into an operational state. Upon completion of any resulting risk treatment the assessor will initiate a subsequent iteration to determine the treated residual risk and record the treatment information within the final IT Risk Assessment Report

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 (more info, page 12), we are also lacking controls in few other domains,
These domains include:

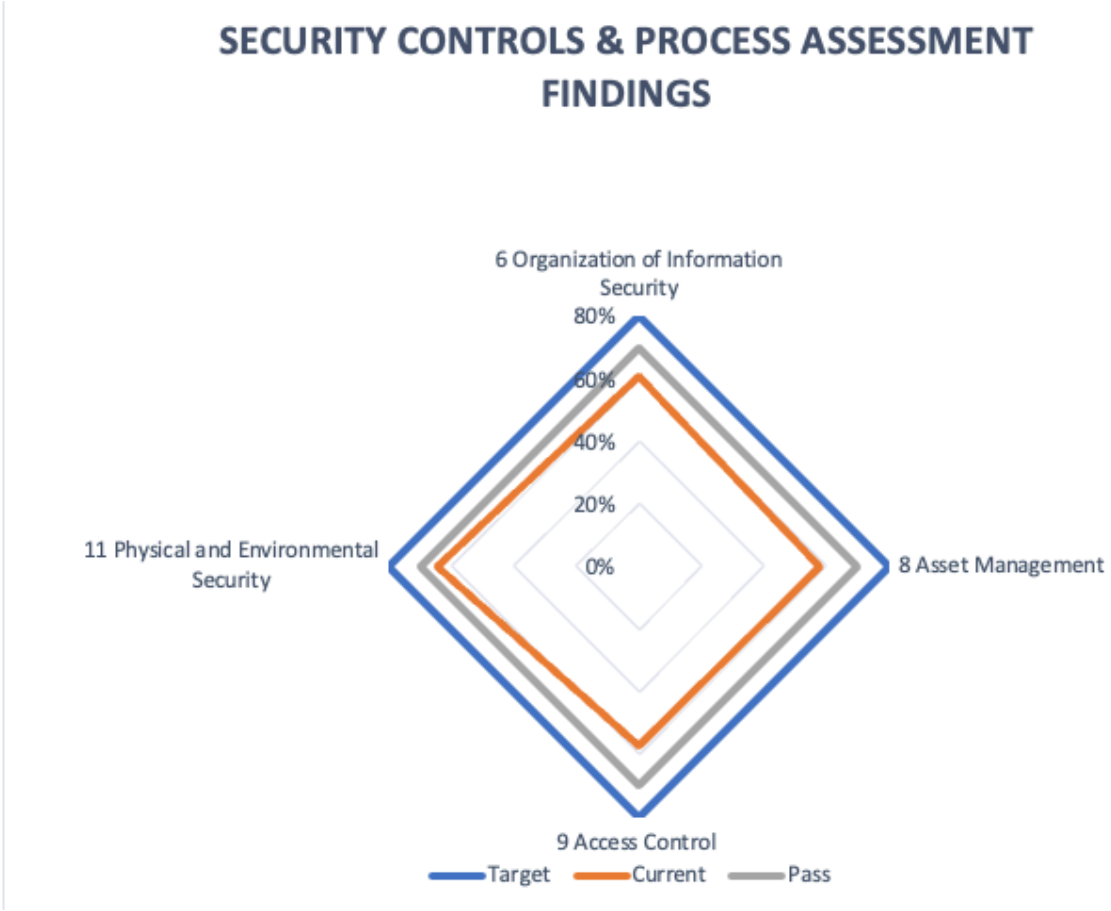
- Organization of Information Security
- Access Controls
- Asset Management
- Physical and Environmental Security

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.

Results of a security controls gap assessments

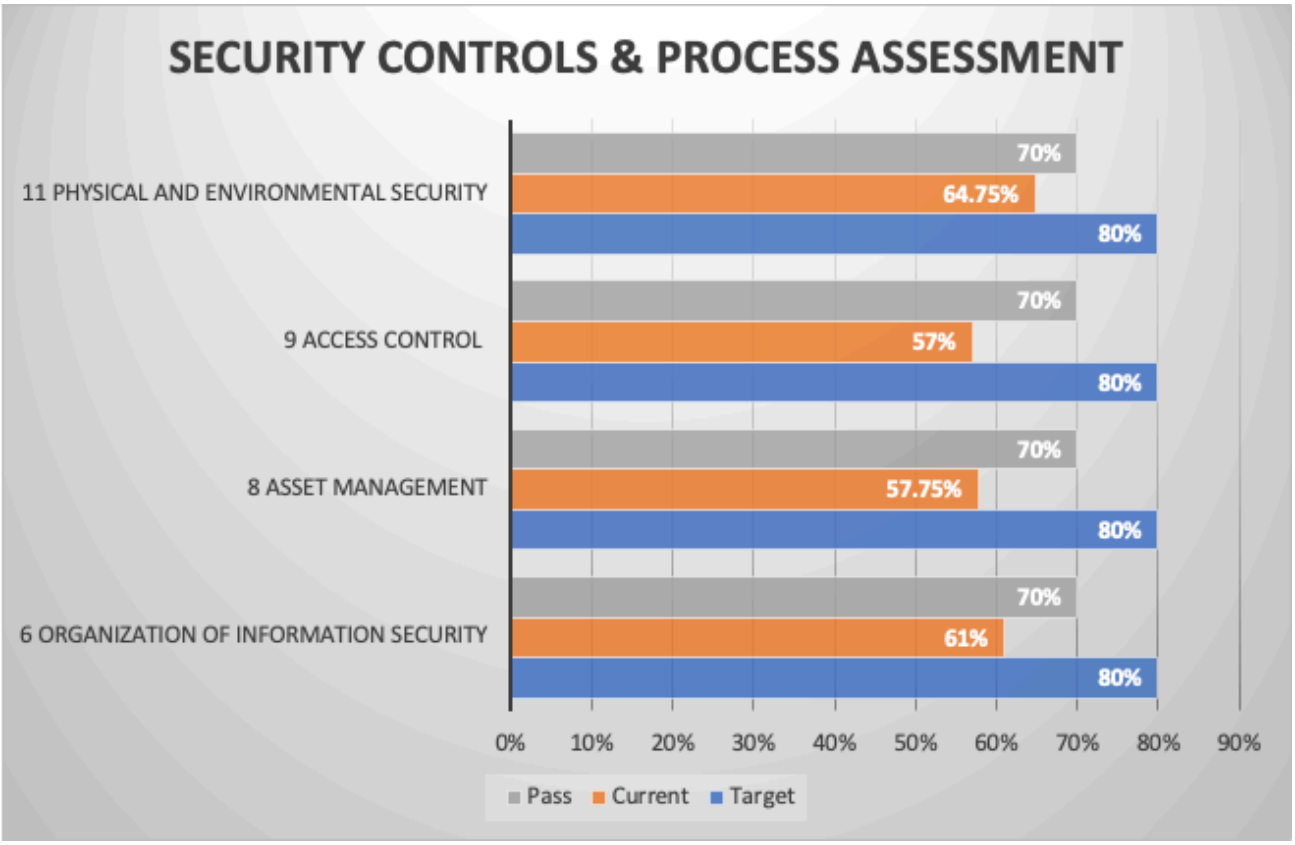
Summary Results – Overview

The following chart provides an overview of ISO Assessment Results by ISO 27002 Domain or control categories.



Summary Results - Scores by Domain

The following chart provides an overview of ISO Assessment Results by ISO 27002 Domain or control categories.

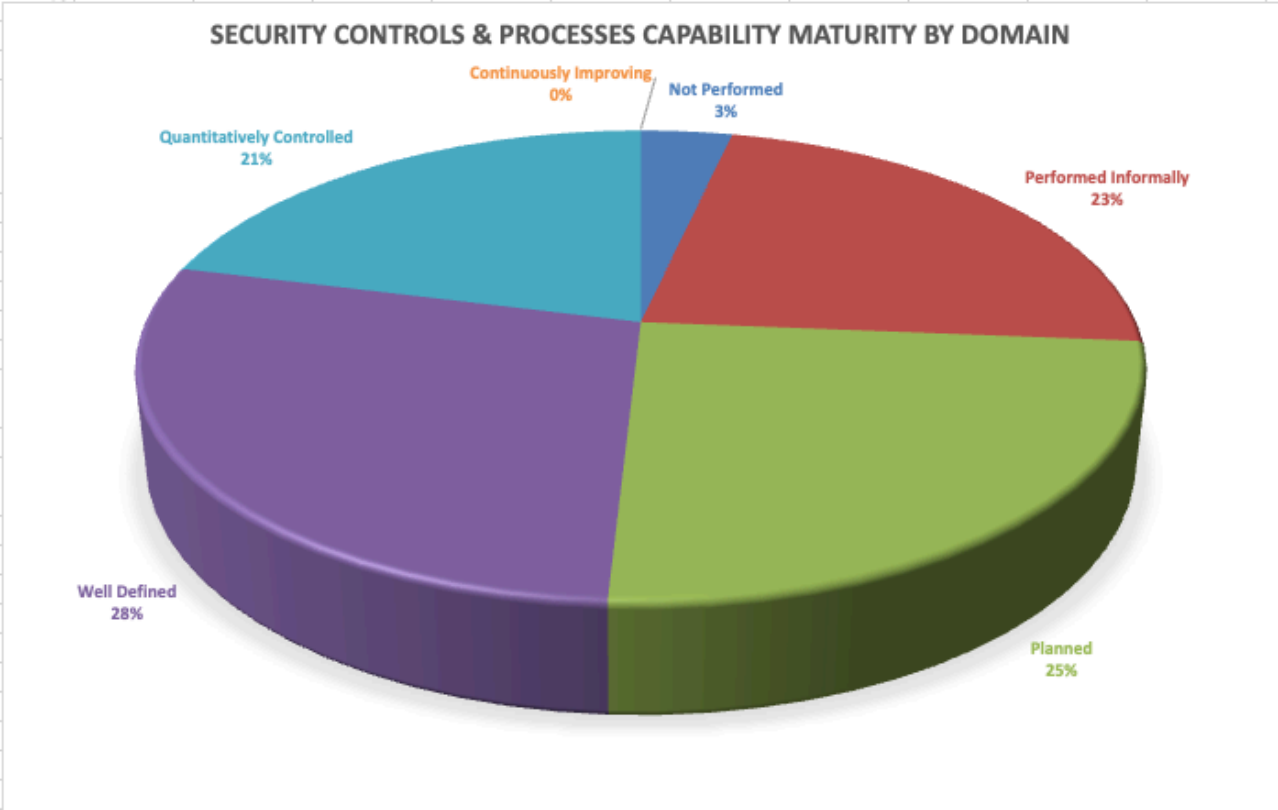


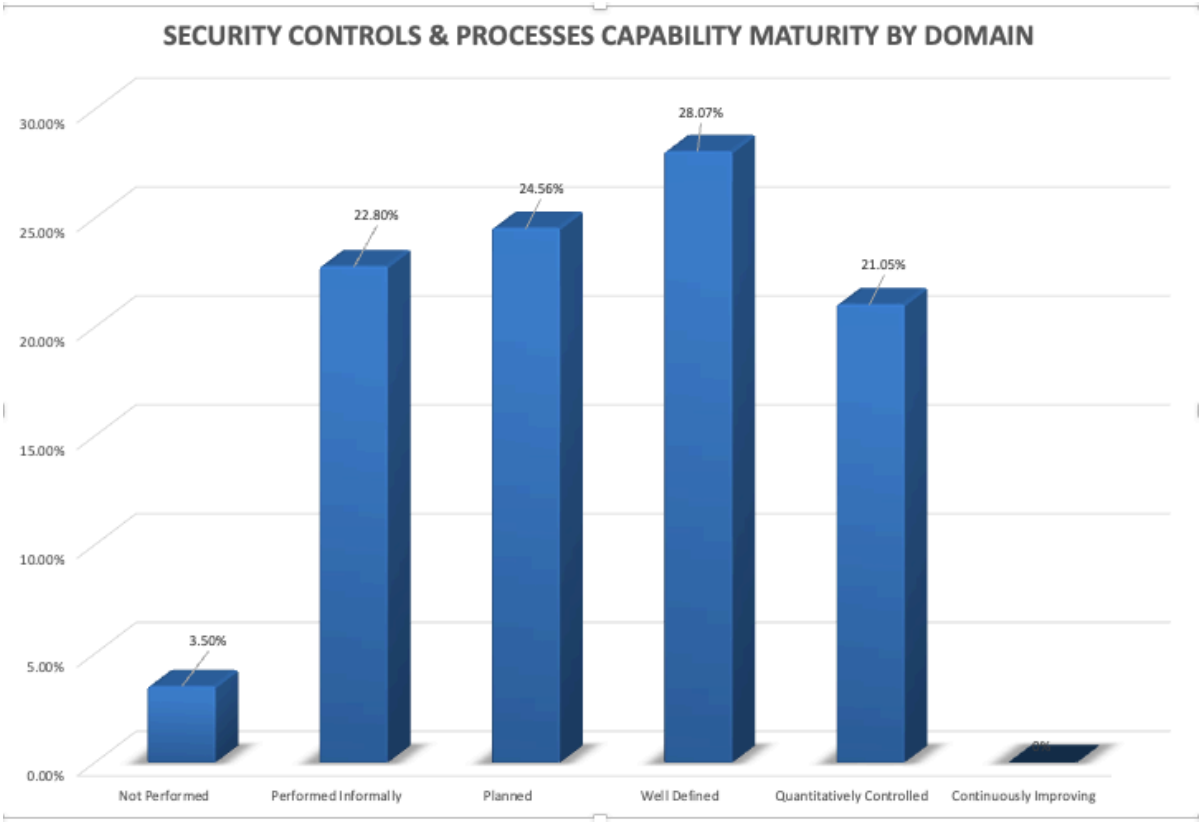
The goal of the ISO 27001 ISMS Compliance Readiness Assessment Project was to identify security weakness that would have make Firearm susceptible to attacks such as unauthorized access to systems and sensitive information disclosure.

Current Security Posture

Security Control Maturity

Overall FIREARM has average security posture with 49% of security controls and processes already in compliance, and some controls are planned (25%), 23% of controls are performed informally and 3% of the controls are "Not performed". To become compliant the remediation effort could take several months.





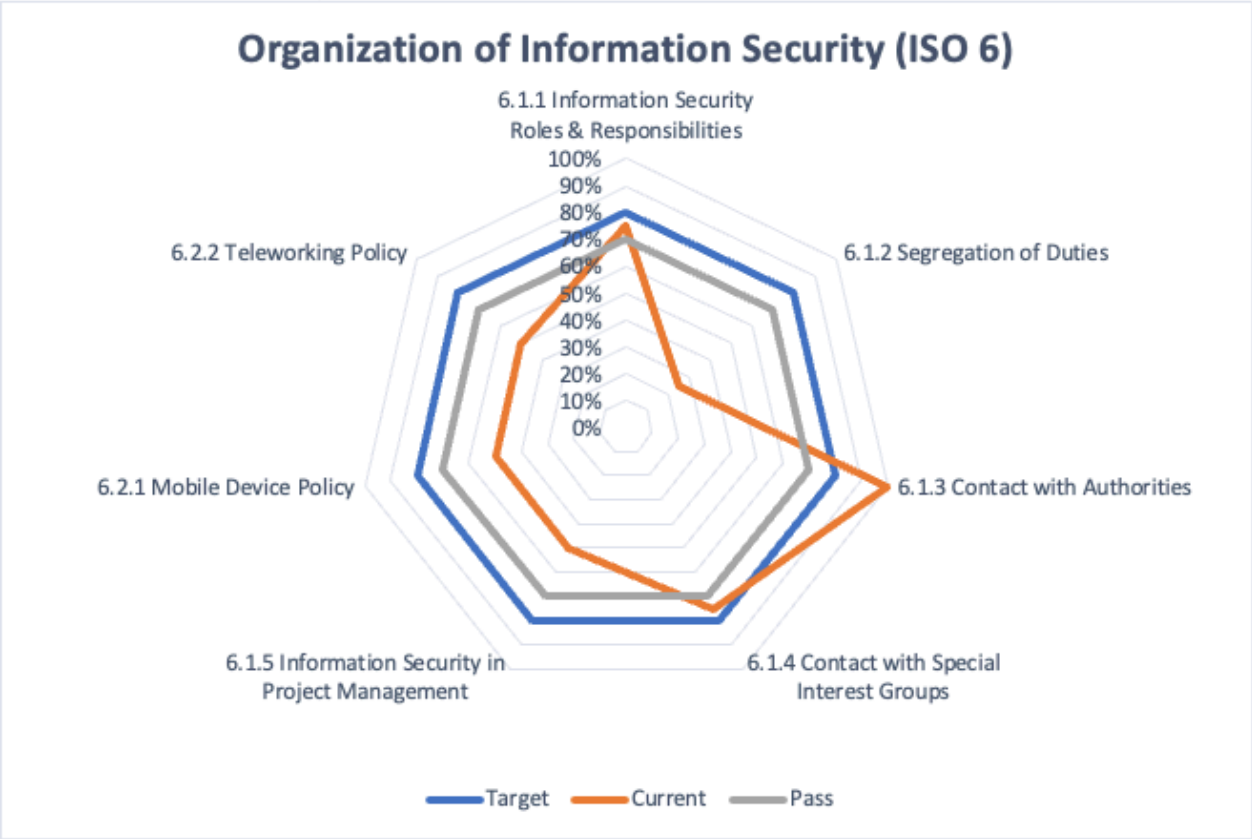
Organization of Information Security (ISO 6)

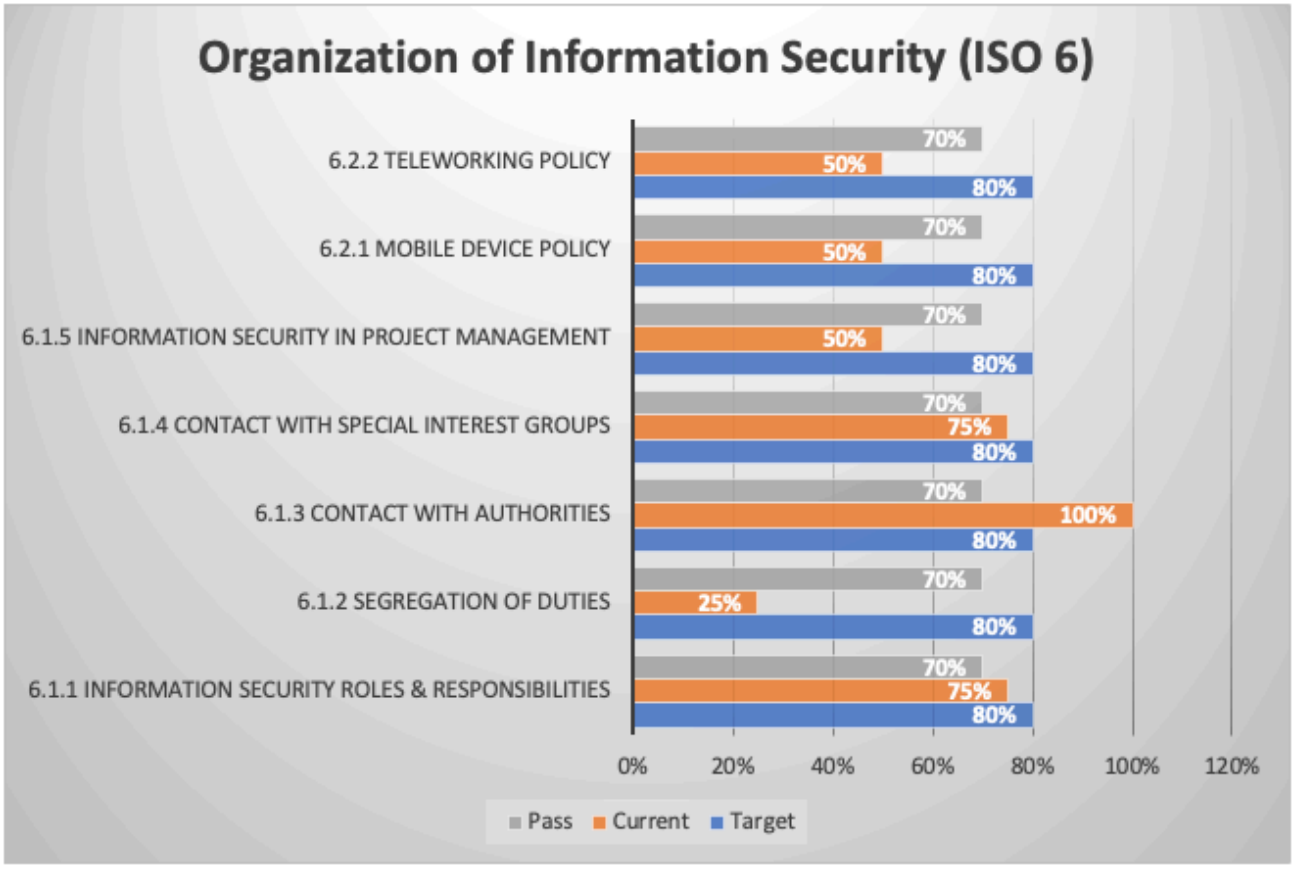
The two major objectives of this domain are

- **6.1 Internal organization**
  Objective: To establish a management framework to initiate and control the implementation and operation of information security within HACME.

- **6.2 Mobile devices and teleworking**
  Objective: To ensure the security of teleworking and use of mobile devices.

Assessment of FIREARM's Organization of Information Security Domain:
FIREARM's Organization of Information Security Domain is in below average condition with only three (3) of the seven (7) sub-domains in compliance and four (4) of the sub-domains that have nonconformities and require corrective action.





Security Control(s) that are in a state of nonconformity and require corrective action:

1. 6.1.2 Segregation of Duties 25%
2. 6.1.5 Information Security in Project Management 50%
3. 6.2.1 Mobile Device Policy 50%
4. 6.2.2 Teleworking Policy 50%

Recommendations:

6.1.2 Segregation of Duties - 25%

Recommendations and Corrective Actions:

a) Conflicting duties and areas of responsibility should be segregated to reduce the risk of unauthorized access and usage of FIREARM's assets

6.1.5 Information Security in Project Management – 50%

Recommendations and Corrective Actions:

a) Conflicting duties and areas of responsibility should be segregated to reduce the risk of unauthorized access and usage of FIREARM's assets

6.2.1 Mobile Device Policy – 50%

Recommendations and Corrective Actions:

a) Agreements should include a clause to establish ownership of business data, authorization to wipe data/device remotely. Procedure to manage stolen mobile devices should have legal and insurance issues.

6.2.2 Teleworking Policy – 50%

Recommendations and Corrective Actions:

a) A policy and measures must be created to include provisions and restrictions to accommodate security requirements for building, friends and family access, right to access equipment to verify security controls.

Asset Management (ISO 8)

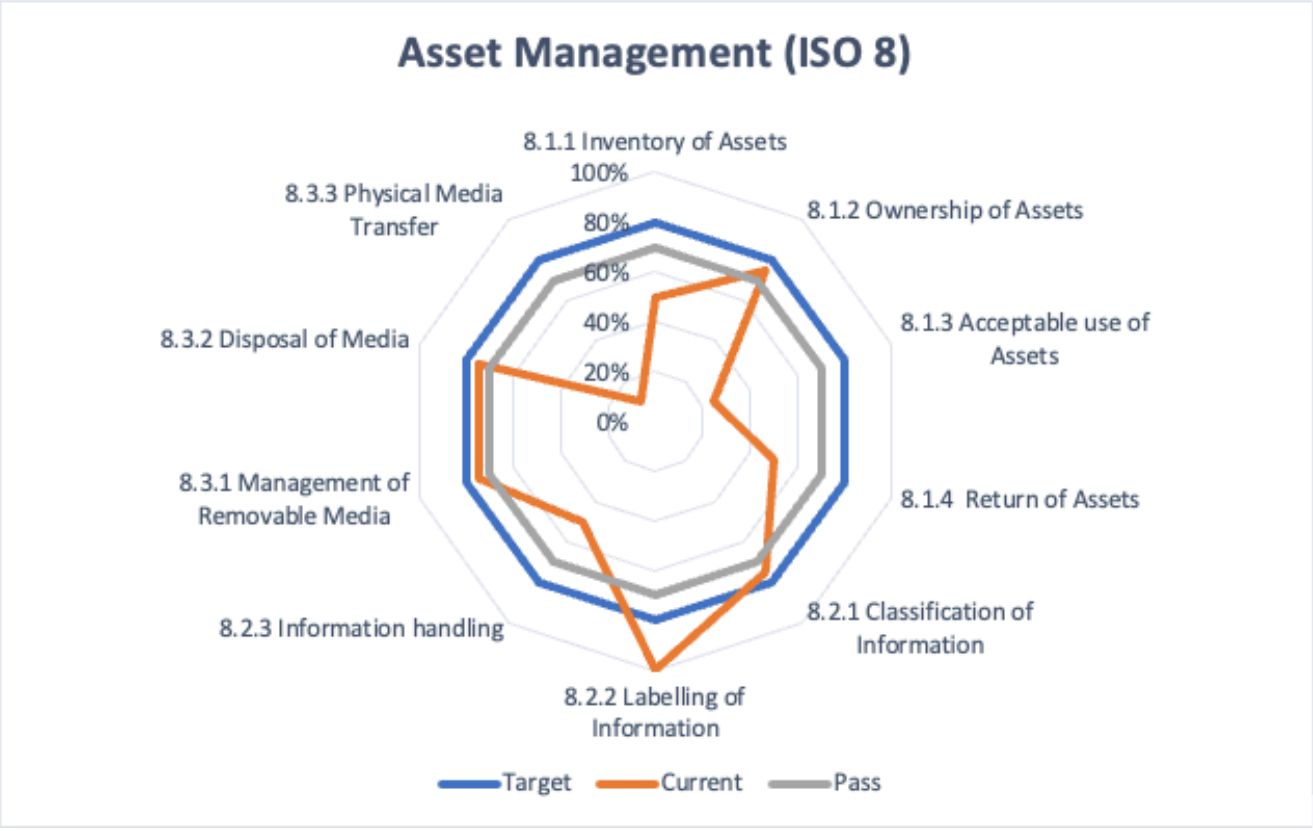
The major objectives of this domain are

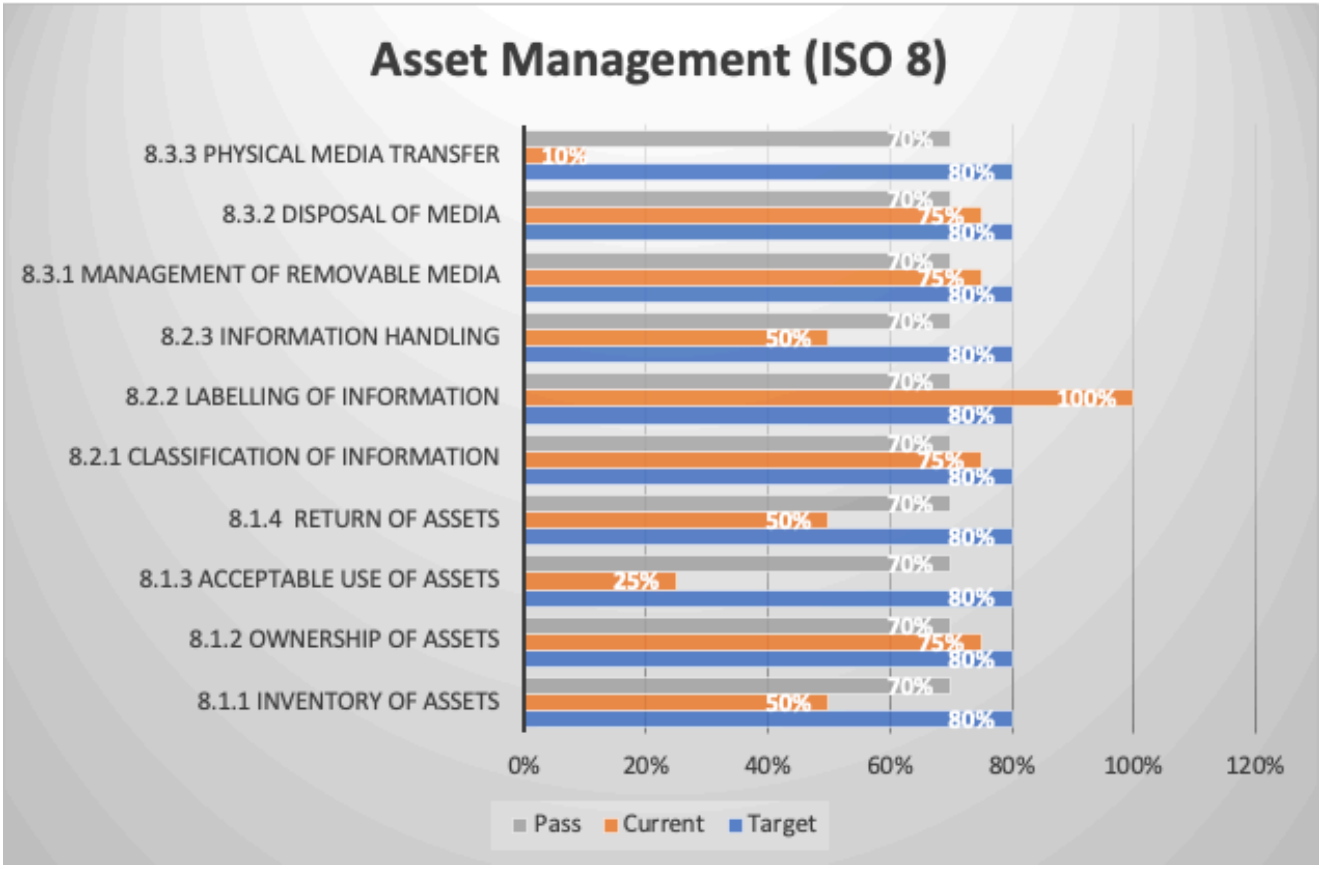
- **8.1 Responsibility for assets**
  Objective: To identify organizational assets and define appropriate protection responsibilities.

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

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

Assessment of FIREARM's Organization of Information Security Domain:
FIREARM's Organization of Information Security Domain 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 Control(s) that are in a state of nonconformity and require corrective action:

1. 8.3.3 Physical Media Transfer 10%
2. 8.1.3 Acceptable use of Assets 25%
3. 8.1.4 Return of Assets 50%
4. 8.2.3 Information handling 50%

8.3.3 Physical media Transfer – 10%

Recommendations and Corrective Actions:

a) Any media containing information should be protected against unauthorized access.

8.1.3 Acceptable use of Assets – 25%

Recommendations and Corrective Actions:

a) "Acceptable use Policy" should be made available to employees, customers and the security guards.

6.1.5 Return of Assets – 50%

Recommendations and Corrective Actions:

a) 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 Information handling – 50%

Recommendations and Corrective Actions:

a) Access restriction to the information about customers must be implemented.

Access Control Management (ISO 9)

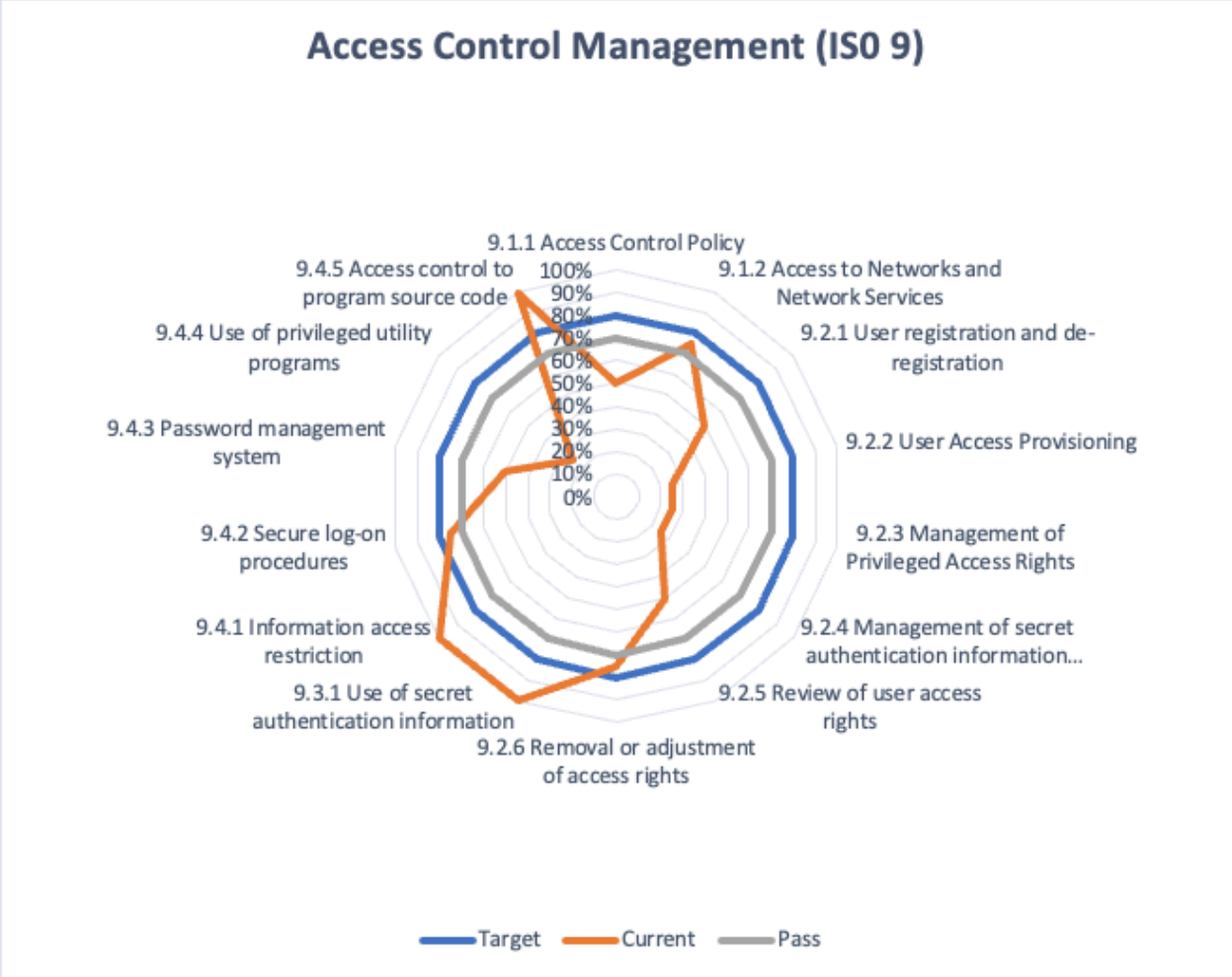
Access Control Management – Primary Objectives

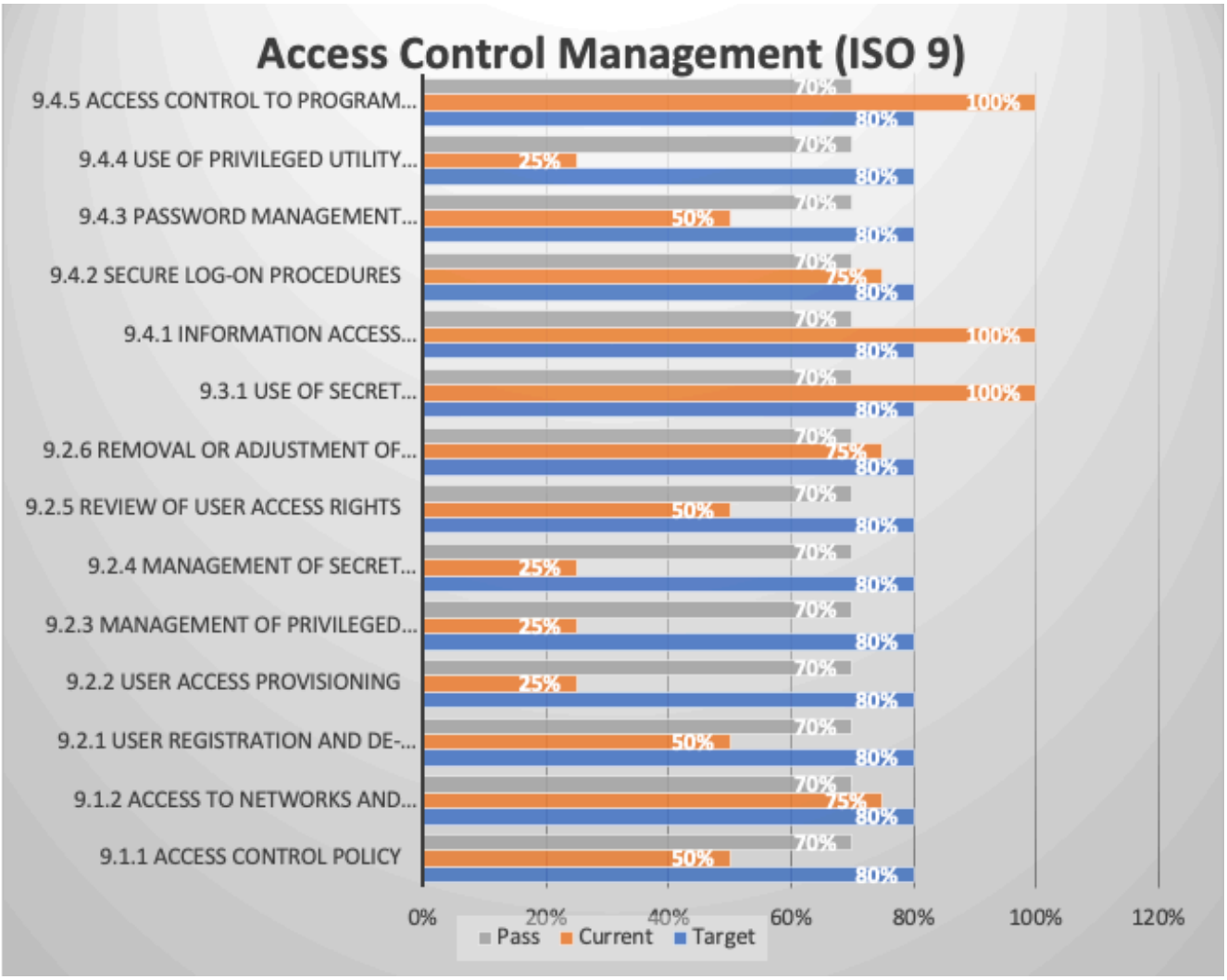
- 9.1 Business requirements of access control
  Objective: To limit access to information and information processing facilities.

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

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

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





Security Control(s) that are in a state of nonconformity and require corrective action:

1. 9.2.2 User Access Provisioning 25%
2. 9.2.3 Management of Privileged Access Rights 25%
3. 9.2.4 Management of secret authentication information 25%
4. 9.4.4 Use of privileged utility programs – 25%
5. 9.2.5 Review of user access rights – 50%

9.2.2 User Access Provisioning – 25%

Recommendations and Corrective Actions:

a) 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 – 25%

Recommendations and Corrective Actions:

a) 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 – 25%

Recommendations and Corrective Actions:

a) 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 – 25%

Recommendations and Corrective Actions:

a) Use of utility programmes should be logged and monitored/reviewed periodically to satisfy auditor requests.

9.2.5 Review of user rights – 50%

Recommendations and Corrective Actions:

a) Amend the procedures frequently and review those periodically for the access rights, roles with privileged access.

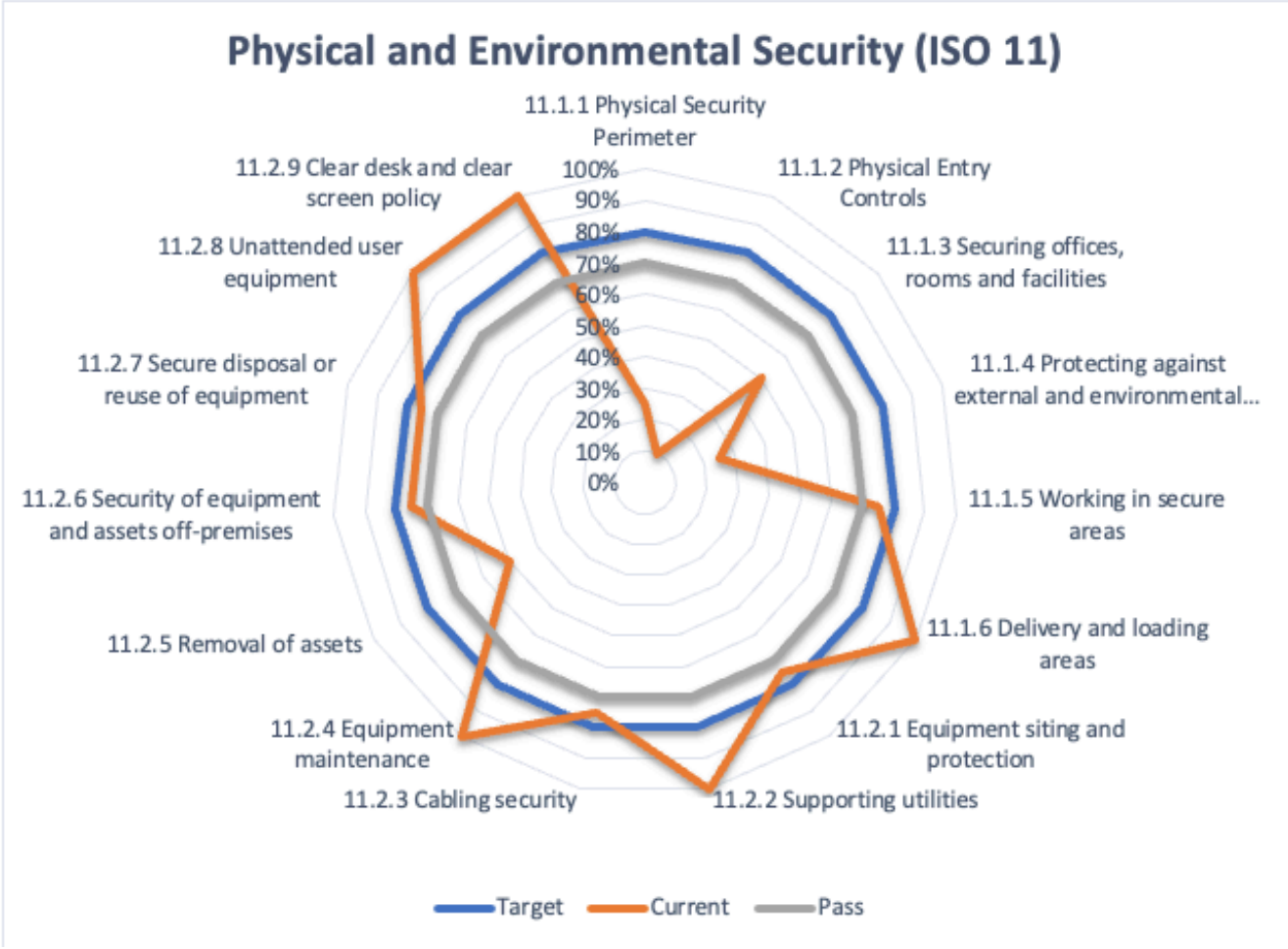
Physical and Environmental Security (ISO 11)

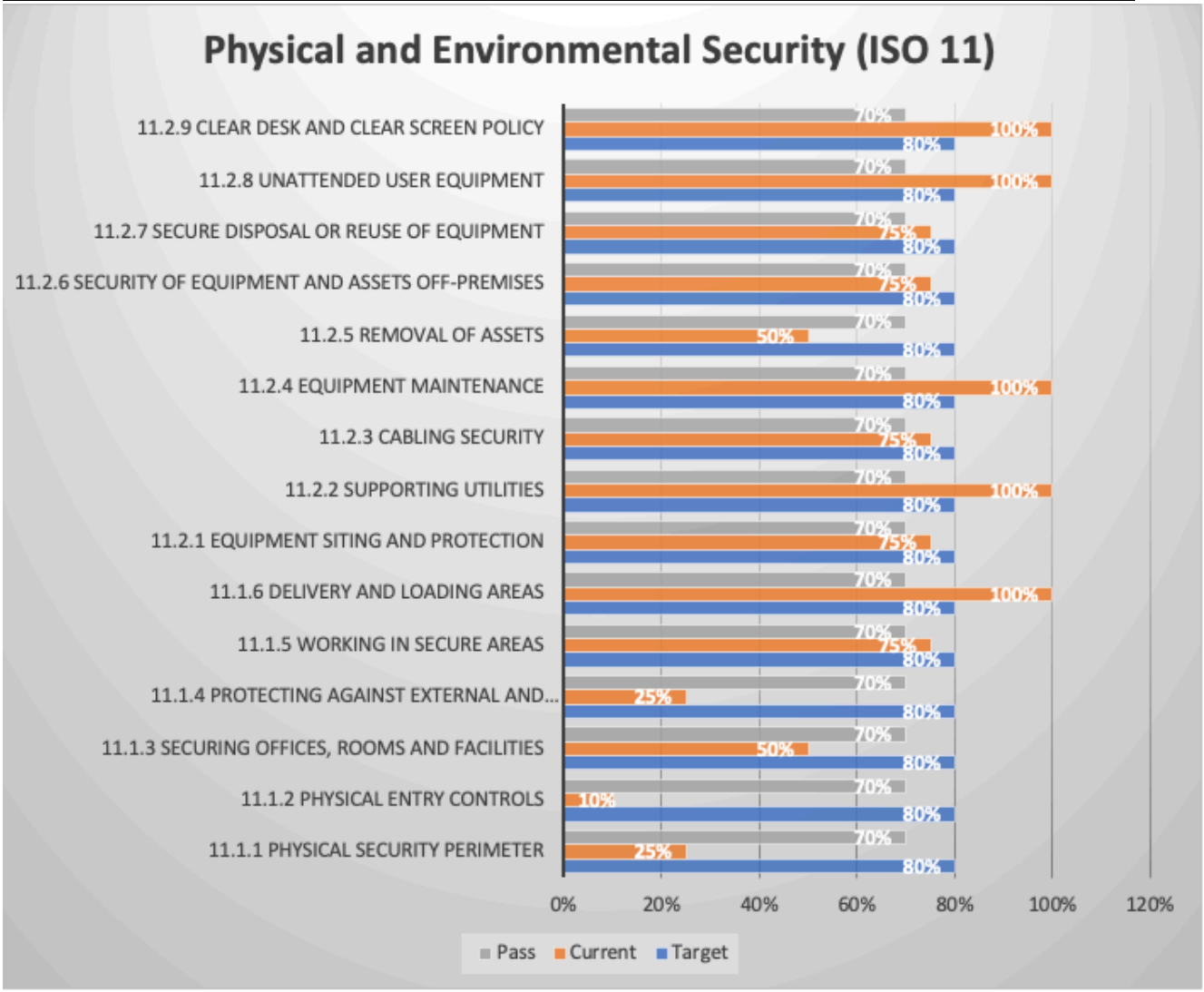
Physical and Environmental Security – Primary Objectives

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

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

Assessment of FIREARM's Physical Security Management:
FIREARM's Organizational Asset Management function is in average condition with ten (10) of the fifteen (15) sub-domains in compliance and five (5) sub-domain that has a nonconformity and require corrective action.





Security Control(s) that are in a state of nonconformity and require corrective action:

1. 11.1.2 Physical Entry Controls 10%
2. 11.1.1 Physical Security Perimeter 25%
3. 11.1.4 Protecting against external and environmental threats 25%
4. 11.1.3 Security offices, rooms, and facilities 50%
5. 11.2.5 Removal of assets 50%

11.1.2 Physical Entry Controls – 10%

Recommendations and Corrective Actions:

a) Along with the existing controls, additional controls like Iris scanner, fingerprint sensors should be placed,

11.1.1 Physical Security Perimeter – 25%

Recommendations and Corrective Actions:

a) FIREARM must establish much more secure areas where the information and assets are placed.

11.1.4 Protecting against external and environmental threats – 25%

Recommendations and Corrective Actions:

a) Get advice from disaster management experts on ways to avoid damage by fire, or natural disasters.

11.1.3 Security offices, rooms, and facilities – 50%

Recommendations and Corrective Actions:

a) Visitors must be escorted to some secure areas.

11.2.5 Removal of assets– 50%

Recommendations and Corrective Actions:

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

Results of a risk assessment

Asset Inventory and Asset Classification

Asset Inventory - Step 1					
Name of Asset	Description of Asset	Type of Asset	Asset Owner (Accountable)	Classification	Location of Asset
Customer Database	Customer Profiles (Name, Address, Birthdate, Current Location, etc.)	Information	VP Opeations	Restricted	Operation Servers
FireArm Mobile Application	Application installed on gaurds' mobile that give them assignments, including a description of the client and their location, and duration of the service.	Software	VP Development	Internal	Application servers
Employee Training and Skills Database	Employee profiles (Name, Job position, Work Experience, Certification, Training, Skills)	Information	VP Database	Internal	Database Servers
Employee Workstation (Asset No. 0086428)	Desktop used by CEO secretary	Equipment	VP IT	Restricted	CEO Secretary
Employee Phone (Asset No. 0086427)	Gaurd's personal mobile device	Equipment	VP IT	Internal	With Employees
Employee Laptop (Asset No. 0086429)	CEO Laptop and mobile	Equipment	VP IT	Restricted	With CEO

Security Impact Analysis

Security Impact Analysis - Step 2							
Name of Asset	Confidentiality	Integrity	Availability	Regulatory	Reputational	Financial	Impact Rating
Customer Database	Very High	High	High	Very High	Very High	Very High	Very High
FireArm Mobile Application	High	Very High	Very High	High	High	High	High
Employee Training and Skills Database	Medium	High	Medium	Medium	Medium	Medium	Medium
Employee Workstation (Asset No. 0086428)	Very High	Very High	Very High	High	High	High	Very High
Employee Phone (Asset No. 0086427)	Very High	High	High	High	High	High	High
Employee Laptop (Asset No. 0086429)	Very High	Very High	Very High	High	Very High	High	Very High

Threats Analysis

	Step 3	Step 3a	Step 4	
Name of Asset	Threat Description	Threat Likelihood	Threat Exposure Rating	Threat Exposure
Customer Database	Compromising confidential information	Likely	High	7
FireArm Mobile Application	Information leakage	Likely	High	6
Employee Training and Skills Database	Fraud	Likely	Medium	5
Employee Workstation (Asset No. 0086428)	Social engineering	Likely	High	7
Employee Phone (Asset No. 0086427)	Theft	Possible	Medium	5
Employee Laptop (Asset No. 0086429)	Social engineering	Likely	High	7

Vulnerability Analysis

	Step 5	
Name of Asset	Vulnerability Description	Vulnerability Severity
Customer Database	Uncontrolled use of information systems	High
FireArm Mobile Application	Insufficient software testing	High
Employee Training and Skills Database	Lack of access control policy	Medium
Employee Workstation (Asset No. 0086428)	Subject to phishing	High
Employee Phone (Asset No. 0086427)	Inadequate replacement of older equipment	High
Employee Laptop (Asset No. 0086429)	Subject to phishing	High

Safeguards Analysis

	Step 6			Step 7
Name of Asset	Primary Safeguard	Primary Safegaurd ID	Primary Safeguard Rating	Residual Risk Rating
Customer Database	7.2.2 Information security awareness, education and training	ISO-013	Medium	High
FireArm Mobile Application	9.4.5 Access control to program source code:	ISO-039	Medium	High
Employee Training and Skills Database	8.1.3 Acceptable use of assets	ISO-018	Medium	Medium
Employee Workstation (Asset No. 0086428)	7.2.2 Information security awareness, education and training	ISO-013	Low	High
Employee Phone (Asset No. 0086427)	6.2.1 Mobile devices policy	ISO-008	Low	High
Employee Laptop (Asset No. 0086429)	7.2.2 Information security awareness, education and training	ISO-013	High	Medium

Recommended Course of Action

Name of Asset	Recommended Course of Action
Customer Database	Create a online module for employees to complete and pass every month for a year. Review this again after a year if we can reduce the frequency of this task.
FireArm Mobile Application	Appliction must be updated constantly.
Employee Training and Skills Database	Access control policy should be developed, monitored and updated. This policy should include who has the authorization to access this data and at what granular level they can access the data.
Employee Workstation (Asset No. 0086428)	Security awareness like phising campaign simulation must be organized freqently, and train employees regarding the latest attacks, safeguards techniques etc
Employee Phone (Asset No. 0086427)	Ensure that the device is encrypted, and Mobile Device Management software is installed and configured according to the Mobile Device Configuration Standard.
Employee Laptop (Asset No. 0086429)	Security awareness like phising campaign simulation must be organized freqently, and train employees regarding the latest attacks, safeguards techniques etc

Risk management strategy

Risk Treatment and 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	4-2-2022	9-1-2022		In progress	3-16-2022
2	FireArm Mobile Application	REDUCE	VP Development		Director Development	Adam Penner	4-3-2022	9-2-2022		Pen test	3-17-2022
3	Employee Training and Skills Database	REDUCE	VP Database		Director Database	Joseph Ruderford	4-4-2022	9-3-2022		In review	3-18-2022
4	Employee Workstation (Asset No. 0086428)	REDUCE	VP IT		Director IT	Christian Bale	4-5-2022	9-4-2022		Hold pending additional information	3-19-2022
5	Employee Phone (Asset No. 0086427)	REDUCE	VP IT		Director IT	Billy Boden	4-6-2022	9-5-2022		In review	3-20-2022
6	Employee Laptop (Asset No. 0086429)	REDUCE	VP IT		Director IT	Chris Gayle	4-7-2022	9-6-2022		In progress	3-21-2022

Expected Security Posture

If the recommendations from the above assessments are implemented as per the best practices, security controls posture will increase. This leads us to a path where we could get ISO certified.

Following are the expected parameters to implement the above recommendations,

Expected Time to Complete	6 – 8 months
Expected Cost	1,56,670 $
Expected Control Posture	49%(Current) -> 75%(Expected)

References

APPENDIX A: Industry Publications and References

FIREARM ITS has set out to utilize a set of industry standards and best practices as guidance towards performing gap assessment, managing cyber security risk. The Risk Management processes incorporate and reference a hybrid of industry standards, guidelines, and practices that are working effectively in our industry today, to contribute to the development of a customized risk framework that will meet the business needs of FIREARM.

The following list documents that have been referenced in the body of this document.

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

- https://www.iso.org/standard/63411.html

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

- https://www.iso.org/standard/72140.html

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

- https://www.iso.org/standard/56742.html

ISO 31000:2018 – Risk Management – Principles and guidelines

- https://www.iso.org/standard/65694.html

ISO 31010:2019 – Risk Management Risk Assessment Techniques

- https://www.iso.org/standard/72140.html

APPENDIX B: 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 C: Other References

Wikipedia
https://en.wikipedia.org/wiki

HACKME Gap analysis and risk assessment Reports

CISO

- https://en.wikipedia.org/wiki/Chief_information_security_officer

Organization Hierarchy

- https://www.hierarchystructure.com/software-company-hierarchy/