Packetlabs

Security Maturity Assessment

ACME Inc.

Dates Assessed: September 13th, 2019 through September 25th, 2019

Report Date: September 25th, 2019

Resource: Richard Rogerson | rogerson@packetlabs.net,
Denis Kucinic | dkucinic@packetlabs.net

Table of Contents

1. Risk Level Descriptions

Risk Ratings

High risk findings pose an immediate risk to corporate assets or sensitive information. Exploitation is possible with minimal effort and exploit code is likely to be publicly available or not required. Exploitation of these items may lead to the compromise of systems, services or sensitive information. It is recommended that these items be actioned as soon as possible.

Medium risk findings pose an indirect risk to information systems. For a compromise of the environment, a significant amount of effort and time is required. Typically, findings with a medium severity do not have publicly available exploit code.

Low risk findings have a small impact on the environment and low likelihood of being exploited. It is generally recommended to address these risks at the lowest priority.

Informational findings are observations made during the assessment which can be addressed with a lower priority. Informational findings typically do not pose a risk to the environment.

2. Executive Summary

Security Controls Assessment

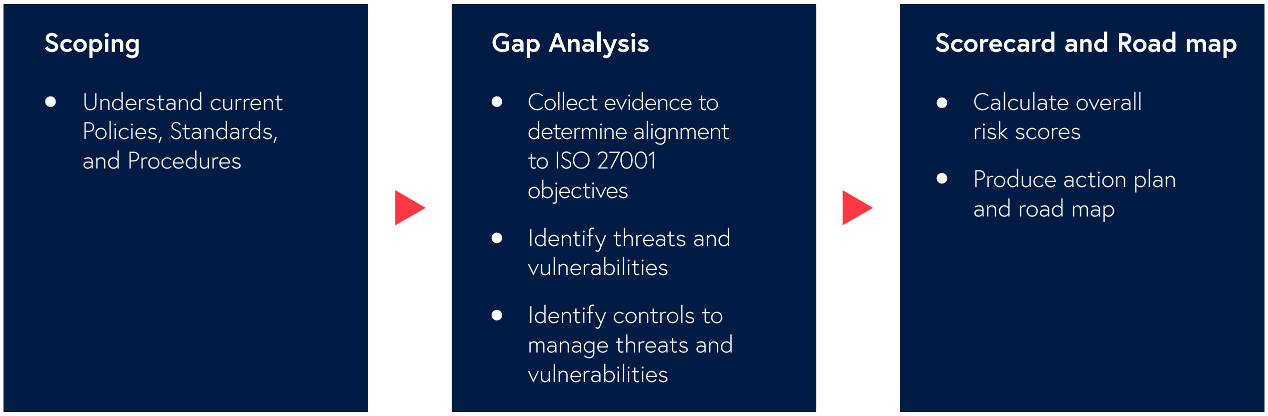
Packetlabs was engaged to perform security controls assessment of ACME Inc. The core objectives of this assessment were to evaluate the current security controls, identify potential risk areas and the effectiveness of the implemented security controls, and lastly, prioritize and facilitate the risk mitigation.

The assessment began on September 13th, 2019 and completed on September 25th, 2019. During this time, the assessment was broken up into three components that included people, process, and technology.

Component	Findings	Overall Risk Level
People	Roles are not clearly defined between Information Technology and Information Security. A dedicated Information Security resource is not available to drive all security initiatives. Security awareness training of all ACME Inc. Personnel must be conducted regularly while including emerging threats. Testing for training compliance through a quiz or phishing exercise is recommended.	! High
Process	Many information security processes are lacking documentation. Those that are documented are lacking compliance by employees. Policies, standards, and procedures are needed to drive governance and compliance across all ACME Inc. Employees.	! High
Technology	Technology deployments exist for many information security controls but are lacking the proper people and processes to utilize them sufficiently. The technologies need to have continuous monitoring and configuration changes to address emerging security threats.	! High

2.1 Approach

Packetlabs assessed the security control capabilities of ACME Inc.'s security program using the ISO/IEC 27001:2013 framework. Packetlabs worked with ACME Inc. To define scope, identify control gaps, generate overall risk scores and develop a remediation road map.
The approach is outlined below:



Scoping

- Understand current Policies, Standards, and Procedures

Gap Analysis

- Collect evidence to determine alignment to ISO 27001 objectives
- Identify threats and vulnerabilities
- Identify controls to manage threats and vulnerabilities

Scorecard and Road map

- Calculate overall risk scores
- Produce action plan and road map

Packetlabs gathered the identified gaps and provided the business risks for each gap, while ensuring that the risks were weighed based on potential impact to ACME Inc.'s business operations.

2.2 The ISO 27001 Framework

The framework assesses ACME Inc. Across multiple security controls and provides a clear indication to areas within the information security program that require additional effort.

The framework assesses the following areas (numbering starts at 5 in ISO27001):

- **Information Security Policies** – Identifies if policies are in place that are regularly reviewed, updated, and approved.
- **Organization of Information Security** – Identifies if the information security team is adequately resourced with clearly outlined responsibilities.
- **Human Resource Security** – Detects if background checks and processes exist for employees prior to employment, during employment, and at termination.
- **Asset Management** – Identifies if assets are appropriately tagged and inventoried and if information is classified according to its sensitivity.

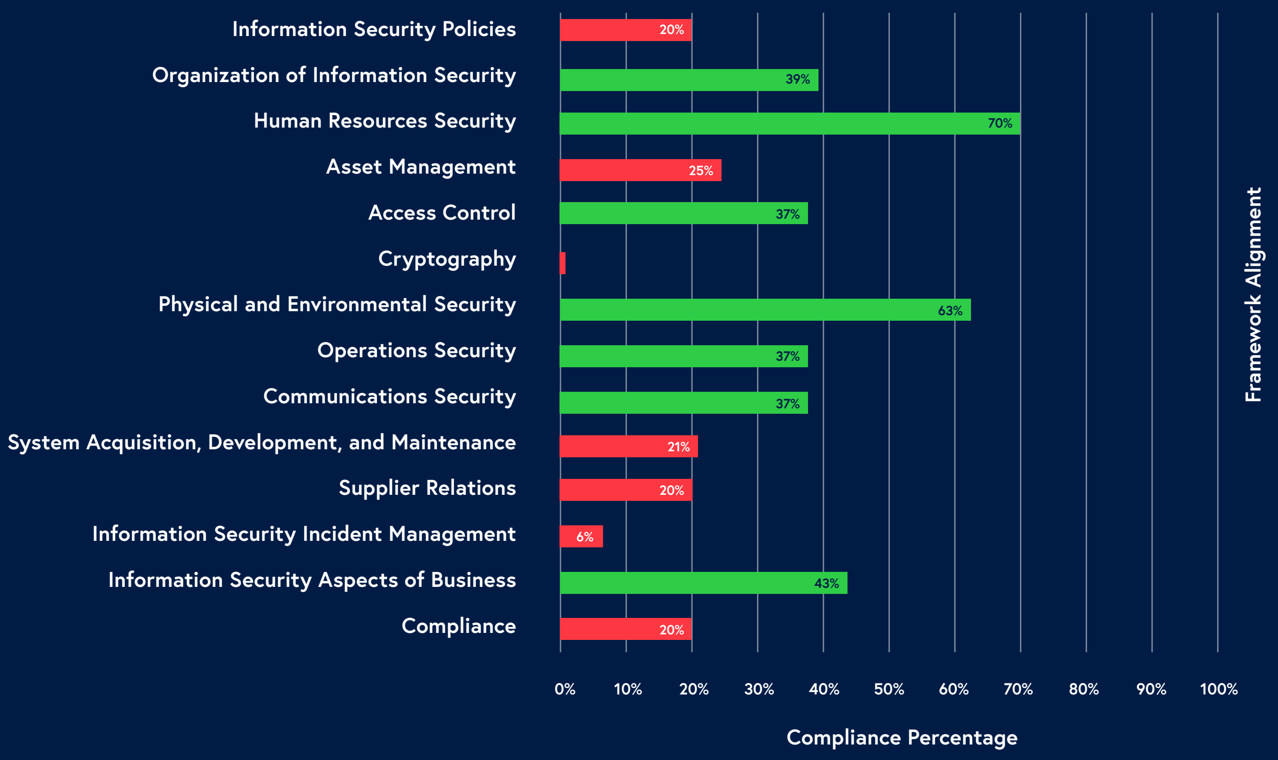
- **Access Control** – Detects if access control mechanisms are in place during all life cycles of the data.
- **Cryptography** – Identifies if strict cryptographic controls are in place to protect sensitive data.
- **Physical and Environmental Security** – assesses the physical environment which includes secure areas and equipment.
- **Operations Security** – Assesses logging and monitoring, backups and recovery, patching, and protection against malware.
- **Communications Security** – Identifies information transfer processes and network security management.
- **Systems Acquisition, Development, and Maintenance** – Assesses secure code development and hardening standards.
- **Supplier Relationships** – Detects if supplier relationships include information security requirements.
- **Information Security Incident Management** – Assesses information security incident response capabilities.
- **Information Security Aspects of Business Continuity Management** – Identifies if redundancies are in place to prevent long outages.
- **Compliance** – Detects if compliance with legal or contractual requirements are being met.

2.3 Score Summary

The framework score across all domains is **31%.**

The score indicates that ACME Inc. requires additional controls to be aligned with ISO/IEC 27001:2013 objectives. ACME Inc. must work to designate adequate resources to policy, standard and procedure creation while ensuring internal and external controls are adequately logged, monitored and actioned upon.

Below are the scores of the existing security controls:



The diagram below dives deeper into the individual controls within each of the higher-level framework pieces above. While some individual pieces within each control have high framework alignment, the overall control when averaged may result in a lower over-all alignment.

5 Information Security Policies

- Management Direction for Information Security

6 Organization of Information Security

- Internal Organization
- Mobile Devices & Telenetworking

7 Human Resources Security

- Prior to Employment
- During Employment
- Termination & Change of Employment

8 Asset Management

- Responsibility for Assets
- Information Classification
- Media Handling

9 Access Control

- Business Requirements for Access Control
- User Access Management
- User Responsibilities
- System & Application Access Control

10 Cryptography

- Cryptographic Controls

11 Physical & Environmental Security

- Secure Areas
- Equipment

12 Operations Security

- Operational Procedures & Responsibilities
- Protection from Malware
- Backup
- Logging & Monitoring
- Control of Operational Software
- Technical Vulnerability Management
- Information Systems Audit Consideration

13 Communications Security

- Network Security Management
- Information Transfer

14 System Acquisition, Development & Maintenance

- Security Requirements for Information Systems
- Development and Suport Processes

15 Supplier Relationships

- Information Security in Supplier Relationships
- Supplier Service Delivery Management

16 Information Security Incident Management

- Management of Security Incidents

17 Information Security Aspects of Business Continuity Management

- Information Security Continuity
- Redundancies

18 Compliance

- Compliance with Legal & Contractual Requirements
- Information Security Reviews

2.4 Business Risk Summary

Packetlabs determined the risk to the business for each of the ISO/EIC 27001:2013 domains and summarized the business risks that have the highest potential impact for each framework item.

5. **Policies do not exist to help govern the information security program across all domains.** Each policy has a purpose. The Information Security Policy needs to engage employees and clearly outlines responsibilities and employee disciplinary actions. Policies are also missing across multiple domains.

6. **Information security roles and responsibilities not clearly defined.** Having clearly defined roles and responsibilities streamlines efficiency by removing unnecessary overlap. ACME Inc. should have an information security team that is not overlapping with any tasks currently conducted by the Physical Security and Information Technology teams.

7. **The onboarding and offboarding of employees is not streamlined or consistent** The onboarding and offboarding process needs to be in a workflow that includes notifying the Information Technology staff to disable accounts and picking up hardware that was issued to the employee.

8. **Media assets (USB, CDs) need to be under stricter controls.** Disabling USB for non-Information Technology staff needs to be considered to prevent the loss of data and spread of malware. [REDACTED]. While malware protection is on the end-points, it only takes one new strain to cause significant impact.

9. **Access permissions are not role based or regularly reviewed.** To ensure consistency across business units, each unit must have identical permissions that are clearly defined in an access control policy and procedure. The access needs to be reviewed on a regular basis to ensure compliance and to ensure terminated employees are not activated in the environment.

10. **Cryptography requirements are missing.** Having a policy that governs cryptography controls ensures all data that is transmitted or stored is secured sufficiently.

11. **Physical security of Information Technology assets not currently formalized.** A procedure needs to be created that includes the removal and disposal of Information Technology assets. The procedure must detail steps on wiping hard drives and the complete process of decommissioning.

12. **Logging of security logs and alerts is not centralized.** A centralized system should be implemented to act as a primary hub for all logs and alerts. The logs and alerts can be tuned and used to notify the required individuals if specific rules are triggered. The purpose of the system could be to identify if data is being exfiltrated and alert if a computer system is compromised. The current deployment of Splunk could be enhanced to incorporate these requirements.

13. **Networking controls while at the ACME Inc. premises.** The current network setup does not limit individuals from gaining access to the ACME Inc. network if physically connected. If an unauthorized party directly connects within the premises, they will be able to maneuver and attempt attacks against internal assets which could lead to a full compromise. It is recommended that controls are introduced to only allow the required systems be allowed on the network.

14. **A formalized change management process is missing.** Change management ensures systems are deployed according to a specific standard and that any system changes go through an approval process that includes Information Technology, Information Security, and if needed, Physical Security.

15. **Supplier relations do not include information security requirements.** Each and every vendor or supplier must be assessed for information security weaknesses. The Physical Security team currently conducts an annual management contract renewal that could be used as an additional gate to conduct the information security assessments. Additionally, new vendors and acquisitions must also have both Information Security and Physical Security review.

16. **Information Security Incident response plans and procedures are not currently implemented.** Incident response plans can assist ACME Inc. if a breach was to occur. By knowing each step required during an incident, all teams can react quickly to remediate the issue and bring the business back to a normal operational state.

17. **Business continuity planning is missing documentation.** A business continuity plan defines all risks to a company's operations (including any weather events) and implements safe guards that are periodically tested and reviewed.

2.5 Recommended Action Plans and Prioritizations

Packetlabs has provided a list of action plans to remediate the identified gaps. The recommendations are prioritized based on the risk and the level of effort to remediate. Each of the action plans will remediate and bring the overall security score higher for each domain.

Task	SO 27001 Gaps Remediated	Priority	Level of Effort
Policy Development Policies are formal statements produced and supported annually. They are used across the entire organization to reflect objectives for the overall security program. These are high-level and do not specify any technical aspects. A policy is a statement of expectation, that is enforced by standards and further implemented by procedures.	5, 8, 9, 11, 13, 15, 18	HIGH	HIGH
Standard Development Standards are mandatory actions or rules that give policies support and direction. These standards specify hardware and software solutions that must be enforced.	10, 18	HIGH	HIGH
Formalize Ticketing System A ticketing system (e.g., Service Now or Sysaid) is required to log all requests and ensure requests are completed in their entirety to prevent any steps in the process from being missed. Each activity requires a new task in the ticketing system.	6, 7, 8, 11, 12, 13, 16	HIGH	HIGH
Vulnerability Management Program A vulnerability management program acts on new threats and addresses newly released vulnerabilities. By prioritizing the vulnerabilities according to their severity within the ACME Inc. environment, risks will be acted upon quickly. The program must be repeatable to ensure vulnerability trends are moving in the correct direction.	12	HIGH	MEDIUM

Contd. on next page

Task	SO 27001 Gaps Remediated	Priority	Level of Effort
Incident Response Program Develop an incident response program to effectively manage security incidents and events. The plan must outline communication requirements along with the handling of all security events.	16	HIGH	MEDIUM
Procedure Development Procedural documents assist standards by providing step-by-step instructions for each task. The procedures can be developed by the teams conducting the tasks and can be as specific as possible.	7, 9, 13	HIGH	MEDIUM
Enhanced Office365 Security Develop and refine the email system by implementing Data Loss Prevention (DLP) and anti-spoofing mechanisms. Audit existing security controls.	14	HIGH	LOW
Information Security Asset Define a position within ACME Inc. that will work to maintain and assist in the implementation of the overall information security program. The resource could be promoted within or acquired externally. CISSP certification should be mandatory.	6	HIGH	LOW
Employee Security Awareness Update training material to include a quiz and current emerging threats using various simulated attacks.	7	HIGH	LOW
Vendor and Supplier Management Include security in all contractual agreements while also creating an organization wide risk management program to assess vendor and supplier risk.	15	MEDIUM	HIGH
Centralized Logging Deploy a centralized logging server that will capture all logs and alerts that are created by all servers.	12	MEDIUM	HIGH
Logical Access Control Improvement Develop and refine logical access controls to secure the network. Doing so will prevent individuals from gaining access to the restricted internal network.	9, 11, 13	MEDIUM	MEDIUM

Contd. on next page

Task	SO 27001 Gaps Remediated	Priority	Level of Effort
USB [REDACTED] Upgrade Identify a new process in which USB [REDACTED] are plugged into a secure environment to prevent the likelihood of a malware infection spreading across ACME Inc.	8, 9, 11, 12, 13, 15, 18	MEDIUM	LOW
Security Audit Review Program Review existing security controls in place regularly to ensure compliance with policies and standards.	18	MEDIUM	LOW
Contractual Compliance Tracking Develop documentation containing all relevant legislative, regulatory and contractual requirements related to security.	18	LOW	LOW
Business Continuity Planning Business Continuity Planning must be enhanced to include information security risks. The BCP must address key risks to the organizations.	17	LOW	LOW

3. Remediation Projects and Roadmap

Remediation Plan

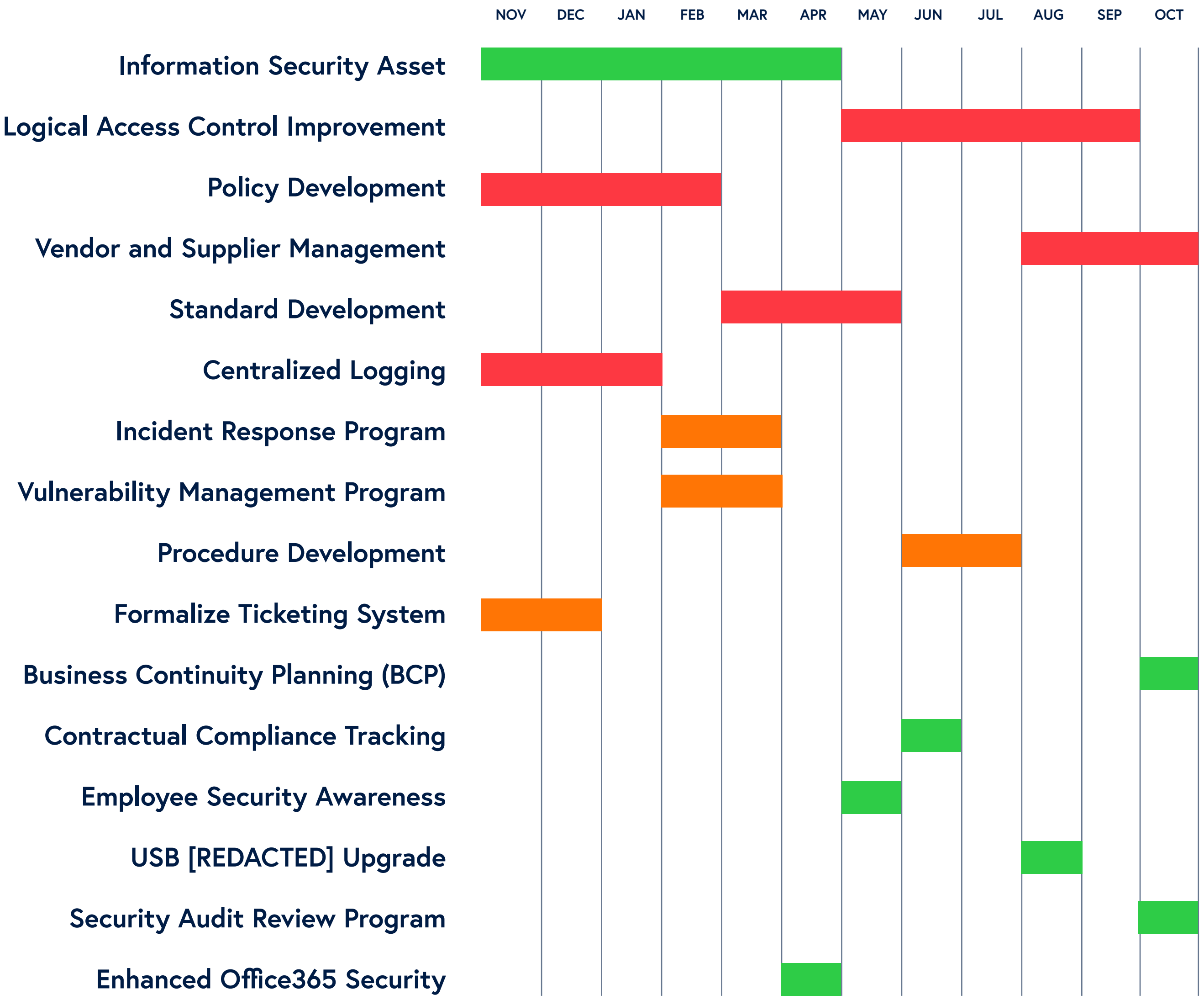
Findings Breakdown

Component	Findings	Overall Risk Level
People	HIGH 3.2.1 Information Security Asset	High
	HIGH 3.2.2 Employee Security Awareness	
Process	HIGH 3.3.1 Policy Development	High
	HIGH 3.3.2 Vulnerability Management Program	
	HIGH 3.3.3 Standard Development	
	HIGH 3.3.4 Incident Response Program	
	HIGH 3.3.5 Procedure Development	
	HIGH 3.3.6 Vendor and Supplier Management	
	MEDIUM 3.3.7 USB [REDACTED] Upgrade	
	MEDIUM 3.3.8 Security Audit Review Program	
	LOW 3.3.9 Contractual Compliance Tracking	
	LOW 3.3.10 Business Continuity Planning (BCP)	
Technology	HIGH 3.4.1 Formalize Ticketing System	High
	MEDIUM 3.4.2 Enhanced Office365 Security	
	MEDIUM 3.4.3 Centralized Logging	
	MEDIUM 3.4.4 Logical Access Control Improvement	

3.1 Remediation Roadmap

The remediation roadmap below was created to assist in developing a timeline. The timeline can be used to identify resource requirements for each project.

The green lines indicate the effort is low but may take long to complete (e.g., acquiring or training an information security asset). The orange lines indicate a medium level of effort while the red lines indicate higher effort.



3.2 People

3.2.1 Information Security Asset

PRIORITY	EFFORT	ISO GAPS REMEDIATED	REMEDIATION TIME
HIGH	LOW	5, 8, 9, 11, 13, 15, 16, 18	6 months

Define a position within ACME Inc. that will work to maintain and assist in the implementation of the overall information security program. The resource could be promoted within or acquired externally. CISSP certification should be mandatory.

The resource may take up to 6 months to acquire externally or if chosen internally, to mature within the role with additional training.

#	Activity	Resource	Effort
1	Create an Information Security role that will govern and enhance the Information Security Program. The role must be separate from Physical Security and Information Technology.	• Senior Management • Human Resources	6 months
2	Once hired, subscribe to special interests' groups to stay relevant on emerging threats.	• Information Security	1 week

3.2.2 Employee Security Awareness

PRIORITY	EFFORT	ISO GAPS REMEDIATED	REMEDIATION TIME
HIGH	LOW	7	1 month

Update training material to include a quiz and current emerging threats using various simulated attacks. Conduct training annually.

#	Activity	Resource	Effort
1	Conduct regular security training to educate staff on emerging threats through live exercises and quizzing. The content must be updated regularly to encompass the current threat landscape.	● Information Security	3 weeks
2	Establish a process to determine adherence to the training material.	● Human Resources	1 week annually
3	Drive security within the business by encouraging employees, contractors and suppliers to apply security in accordance with established policies and procedures. If they see something suspicious, they should report it.	● Senior Management ● Information Security	Monthly

3.3 Process

3.3.1 Policy Development

PRIORITY	EFFORT	ISO GAPS REMEDIATED	REMEDIATION TIME
HIGH	LOW	5, 8, 9, 11, 13, 15, 16, 18	4 months

Policies are formal statements produced and supported annually. They can be used across the entire organization to reflect objectives for the overall security program. These are high-level and do not specify any technical aspects. A policy is a statement of expectation, that is enforced by standards and further implemented by procedures.

These policies must be reviewed annually to ensure they are current and communicated to all employees. Any changes to them must be highlighted to all employees.

#	Activity	Resource	Effort
1	Enhance the current Information Security Policy to include incident management, supplier management, and cryptography in addition to clearly defining information security roles, responsibilities and enforcements.	● Information Security ● Senior Management	1 week
2	Develop an Asset Management Policy that assists in the ownership, maintenance and handling of all physical Information Technology assets.	● Information Security ● Senior Management	1 week
3	Develop an Acceptable Use Policy to set the requirements for browsing the internet, using personal devices, email and social media.	● Information Security ● Senior Management	2 weeks
4	Develop an Access Control Policy to govern the authorization and authentication requirements for viewing data.	● Information Security ● Senior Management	1 week
5	Develop a Supplier Relationship Policy to set information security requirements for the screening, agreements, access control, monitoring and termination.	● Information Security ● Supplier Relations	2 weeks
6	Develop an Information Transfer Policy to set requirements for electronic communication channels and relations with external parties while dealing with sensitive transfers.	● Information Security ● Senior Management	1 week
7	Enhance existing Teleworking Policy to address associated security risks (e.g., who may telework, which services are available for teleworkers, which information can be accessed, how devices should be protected).	● Information Security ● Senior Management	1 week
8	Develop a Removeable Media Policy to minimize exposure of sensitive information.	● Information Security	1 week

#	Activity	Resource	Effort
9	Develop a Cryptography Policy which provides guidance on the use of encryption and algorithms to be used when protecting and transmitting data both on and off premises. This must govern the entire lifecycle of cryptographic keys.	• Information Security	1 week
10	Develop a Backup Policy to ensure backup copies are created at defined intervals and regularly tested.	• Information Security • Information Technology	1 week
11	Develop a Forensic Readiness Policy to be able to collect, preserver, protect and analyze digital evidence that can be effectively used in legal matters, security investigations, disciplinary actions, or in a court of law.	• Information Security • Information Technology	4 weeks
12	Develop a Clean Desk Policy that will enforce keeping desks clear of sensitive information.	• Information Security	1 week

3.3.2 Vulnerability Management Program

PRIORITY	EFFORT	ISO GAPS REMEDIATED	REMEDIATION TIME
HIGH	MEDIUM	12	2 months

A vulnerability management program acts on new threats and addresses newly released vulnerabilities. By prioritizing the vulnerabilities according to their severity within the ACME Inc. environment, risks will be acted upon quickly. The program must be repeatable to ensure vulnerability trends are moving in the correct direction. The process needs to align to the PDCA model where:

- Plan – risks are assessed, risk treatment plans are created (patching process), and risks are accepted (if a patch cannot be deployed)
- Do – implement patching and mitigating strategies

- **Check** – continual monitoring and review of risks (on-going scans)

- **Act** – maintain and improve the process

#	Activity	Resource	Effort
1	Identify scanning tool or solution (e.g., Qualys)	• Information Security	1 week
2	**Conduct Vulnerability Scanning** **1.** Identify assets and categorize according to severity. **2.** Scan assets. **3.** Rank risks according to business risk. **4.** Patch the vulnerabilities (test first). **5.** Create a trending report to present to management.	• Information Security • Information Technology • Asset Business Owner	Monthly
3	Develop a Risk Acceptance form for legacy systems where business owners will sign and accept the risk to those systems being unprotected.	• Information Security	Monthly
4	Develop a process in which publicly accessible web applications and services are tested thoroughly on a predefined basis to ensure secure coding practices are in place.	• Information Security	Annually

3.3.3 Standard Development

PRIORITY	EFFORT	ISO GAPS REMEDIATED	REMEDIATION TIME
HIGH	HIGH	10, 18	3 months

Standards are mandatory actions or rules that give policies support and direction. These standards specify hardware and software solutions that must be enforced. For example, the Cryptography Standard will discuss specific details about cipher key strengths and lengths.

These Standards must be reviewed annually to ensure they are current and communicated to all employees. Any changes to them must be highlighted to all employees.

#	Activity	Resource	Effort
1	Develop a Cryptography Standard which outlines data protection while in transit, rest and in use while setting the minimum requirements for the encryption algorithms.	● Information Security ● Senior Management	2 weeks
2	Develop an Access Control Standard which outlines authorization, authentication, and entitlement review requirements.	● Information Security ● Senior Management	1 week
3	Develop a Threat and Vulnerability Management Standard to detail vulnerability monitoring, scanning, penetration testing, and remediation.	● Information Security	1 week
4	Develop an Information Classification Standard to define the classification of data.	● Information Security ● Senior Management	1 week
5	Develop a Decommissioning Standard which defines how assets are to be disposed of or reused.	● Information Security	1 week
6	Develop an Information Transfer Standard to define methods of transferring data externally.	● Information Security ● Senior Management	1 week
7	Develop a Hardening Standard for all systems. New systems being implemented in the environment need to abide by the standard.	● Information Security	1 week
8	Develop a Secure Software Development Life Cycle (S-SDLC) that all developed code must abide by. While the Security document provided by Stassy Gallant speaks to controls, it needs to be refined to speak to the building, quality assurance and security testing prior to deploying to production.	● Information Security	2 weeks

3.3.4 Incident Response Program

PRIORITY	EFFORT	ISO GAPS REMEDIATED	REMEDIATION TIME
HIGH	MEDIUM	16	2 months

Develop an incident response program to effectively manage security incidents and events. The plan must outline communication requirements along with the handling of all security events. For example, if ransomware was to strike the environment, the steps to detect, contain, remediation and recover will be clearly defined. Doing so prepares each and every team affected.

#	Activity	Resource	Effort
1	Develop an incident response program with clear roles, responsibilities and processes for reporting and handling security incidents (including contact with relevant authorities). The program must include lessons learned to prevent or reduce the probability of another incident.	• Information Security • Senior Management	2 weeks
2	Define and document a process that will be used by employees and suppliers for reporting security incidents.	• Information Security • Senior Management	2 weeks
3	Develop and communicate expectations for reporting security weaknesses and events to employees and suppliers.	• Information Security • Senior Management	1 week
4	Implement an annual tabletop exercise to test the effectiveness and efficiency of the incident response program.	• Information Security • Senior Management	2 weeks

3.3.5 Procedure Development

PRIORITY	EFFORT	ISO GAPS REMEDIATED	REMEDIATION TIME
HIGH	MEDIUM	7, 9, 13	2 months

Procedural documents assist standards by providing step-by-step instructions for each task. The procedures can be developed by the teams conducting the tasks and can be as specific as possible. For example, the onboarding and offboarding can have detailed steps for the Information Technology team to disable active directory, email, VPN, and any other services the user has.

#	Activity	Resource	Effort
1	Develop a procedure for onboarding and offboarding employees to ensure access is granted on a need-to-know basis and revoked upon departure. This must include hardware any other company owned assets.	• Information Security • Information Technology • Human Resources	1 week
2	Develop an Asset Management procedure which is used to onboard and offboard assets.	• Information Security • Information Technology	1 week
3	Develop a Change Management procedure where any changes the network or environment must under-go review and approvals.	• Information Security • Information Technology	1 week
4	Develop an Information Classification procedure that each employee must abide by when creating new documents.	• Information Security • Senior Management	1 week
5	Develop a Backup procedure that details how each unique backup file is recovered. It must include compliance with relevant legal frameworks.	• Information Technology	4 weeks
6	Develop a Media Handling procedure on how USBs and CDs are to be used, transported, and disposed of.	• Information Security	1 week

#	Activity	Resource	Effort
7	Develop a Capacity Management procedure that is used to ensure capacity is available for maintenance and new projects.	• Information Technology	1 week
8	Develop procedural documents for all tasks conducted by Information Security so that a new employee could pick up tasks more easily.	• Information Security	Unknown
9	Develop an Incident Response procedure for reporting information security weaknesses that is communicated to the entire organization. The process must have a task for reviewing and addressing the reports in a timely manner.	• Information Security	1 week
10	Develop a Clean Desk Procedure that involves monthly checks for locked drawers and insecure sensitive information.	• Information Security	1 week
11	**Develop an Equipment Procedure that covers:** • Securing assets while off-site • Securing unattended equipment • Equipment reuses • Data wiping • Decommissioning	• Information Security • Information Technology	1 week
12	Develop a Secret Authentication Procedure that will be used to provide users with new authentication information (e.g., passwords). The procedure should verify the identity of the user prior to providing authentication information.	• Information Security • Information Technology	1 week

3.3.6 Vendor and Supplier Management

PRIORITY	EFFORT	ISO GAPS REMEDIATED	REMEDIATION TIME
MEDIUM	HIGH	15	3 months

Include security in all contractual agreements while also creating an organization wide risk management program to assess vendor and supplier risk. The current annual management review that updates suppliers on any new health and safety standards can be improved to include all the information security requirements.

#	Activity	Resource	Effort
1	Update vendor and supplier agreements to include requirements for notification in case of a security breach.	• Information Security • Vendor Management	2 weeks
2	Establish a set of security controls to be adhered to by all vendors and suppliers. Include these controls in agreements.	• Information Security • Vendor Management	4 weeks
3	Develop a process to notify vendors and suppliers to any changes to information security policies.	• Information Security • Vendor Management	2 weeks
4	Develop a process to review suppliers for adherence to information security requirements. Include the signing of confidentiality and non-disclosure agreements.	• Information Security • Vendor Management	4 weeks

3.3.7 USB [REDACTED] Upgrade

PRIORITY	EFFORT	ISO GAPS REMEDIATED	REMEDIATION TIME
MEDIUM	LOW	8, 9, 11, 12, 13, 15, 18	1 month

Identify a new process in which USB [REDACTED] are plugged into a secure environment to prevent the likelihood of a malware infection spreading across ACME Inc.

#	Activity	Resource	Effort
1	Develop an Information Transfer procedure which clearly defines the step-by-step process for receiving data from [REDACTED] where the USB is plugged into a segmented, secure zone.	• Information Security	4 weeks

3.3.8 Security Audit Review Program

PRIORITY	EFFORT	ISO GAPS REMEDIATED	REMEDIATION TIME
MEDIUM	LOW	18	1 month

Review existing security controls in place regularly to ensure compliance with policies and standards.

#	Activity	Resource	Effort
1	Develop a technical review process to identify compliance with the existing security policies and standards. Reviews should be run semi-annually and include information systems and security controls.	• Information Security	2 weeks

#	Activity	Resource	Effort
2	Conduct a password policy audit to ensure compliance with password policy.	• Information Security	2 weeks
3	Conduct a scan (using Card Recon) to ensure sensitive documents are not in unfamiliar places and are labelled according to the Information Classification Standard.	• Information Security	1 day
4	Conduct a firewall review to ensure rules are as expected.	• Information Security	1 week
5	**Conduct a user entitlement review to ensure:** • permissions for each user and role are as documented within each application. • terminated employees are no longer active in any systems. • privileged programs are only provided to individual for the length of time they require it • unlicensed software is not used • role based access controls are as intended where users only have access to what they need access to	• Information Security	1 week
6	Assess if secure transactions are performed and stored in a secure internal environment and that they meet all jurisdictional legal, regulatory and compliance requirements.	• Information Security	1 week

3.3.9 Contractual Compliance Tracking

PRIORITY	EFFORT	ISO GAPS REMEDIATED	REMEDIATION TIME
LOW	LOW	18	2 months

Develop documentation containing all relevant legislative, regulatory and contractual requirements related to information security and physical security.

#	Activity	Resource	Effort
1	Develop a document that contains all regulatory and contractual requirements alongside the approach to meet these requirements.	• Senior Management • Information Security	1 week
2	Develop a document that is used to ensure the privacy and protection of personally identifiable information (PII) to abide with relevant legislation (e.g., PIPEDA)	• Senior Management • Information Security	1 week
3	Ensure contracts with external third parties (e.g., [REDACTED]) detail the requirements for securing business information in transfer (e.g., [REDACTED] USBs should not contain malware and they need to be held accountable)	• Information Security	1 week
4	Ensure supplier access to information assets and infrastructure is controlled and monitored.	• Information Security • Physical Security	1 week

3.3.10 Business Continuity Planning (BCP)

PRIORITY	EFFORT	ISO GAPS REMEDIATED	REMEDIATION TIME
LOW	LOW	17	1 month

Business Continuity Planning must be improved to include information security risks. The BCP must address key risks to the organizations, such as:

1. What happens when a major data centre with your information and applications in it becomes unavailable?

2. What happens when a major data breach occurs, a ransomware attack is made or a key person in the business is out of action.

#	Activity	Resource	Effort
1	Develop a document that assists in the implementation and maintenance of information security during a disruptive situation.	• Senior Management • Information Technology • Information Security	4 weeks
2	Verify, review and evaluate BCP plan annually	• Senior Management • Information Technology • Information Security	Annually

3.4 Technology

3.4.1 Formalize Ticketing System

PRIORITY	EFFORT	ISO GAPS REMEDIATED	REMEDIATION TIME
HIGH	HIGH	6, 7, 8, 11, 12, 13, 16	2 months

A ticketing system (e.g., Service Now or Sysaid) is required to log all requests and ensure requests are completed in their entirety to prevent any steps in the process from being missed. Each activity requires a new task in the ticketing system.

This requires support from all levels of management to roll out.

#	Activity	Resource	Effort
1	**Security in Project Management** New projects and activities must make a request for an Information Security resource.	• Project Management • Senior Management • Information Security	1 week
2	**Onboarding and Offboarding** All request must go through the appropriate approvals to offboard and onboard employees. (e.g., hiring manager). Additionally, a task for each team required to onboard and offboard must be created (e.g., information technology to add users to active directory)	• Information Technology • Human Resources • Information Security	1 week
3	**Change Management** All new configuration changes, additions or removals of assets and software must go through appropriate approvals, reviews (hardening and capacity compliance checks) and changes on asset tracking software.	• Information Technology • Information Security	2 weeks
4	**USB [REDACTED] Management** All requests to update [REDACTED] must be ticketed and logged.	• Physical Security • Information Security • Information Technology	1 week

#	Activity	Resource	Effort
5	**New Software Installation** New software requests where individuals require software that is out of the approved software list must be ticketed, approved (by manager and information security), and logged.	● Information Technology ● Information Security	1 week
6	**Incident Management** Any security incidents must be alerted upon and ticketed for forensics time keeping purposes.	● Information Technology ● Information Security	1 week
7	**Removeable Media** A ticket must be created and approved when any sensitive data is taken off-site.	● Information Technology ● Information Security	1 week

3.4.2 Enhanced Office365 Security

PRIORITY	EFFORT	ISO GAPS REMEDIATED	REMEDIATION TIME
HIGH	LOW	14	1 month

Develop and refine the email system by implementing Data Loss Prevention (DLP) and anti-spoofing mechanisms.

#	Activity	Resource	Effort
1	Complete an audit review of the Office365 environment.	● Information Security ● Vendor Management	1 week
2	Refine existing Office365 controls to enable SPF, DKIM, DMARC, and a tag that specifies if an email came from an external address.	● Information Security ● Vendor Management	2 weeks
3	Implement a Data Loss Prevention system that will monitor and prevent the transfer of sensitive files.	● Information Security ● Senior Management	1 week

3.4.3 Centralized Logging

PRIORITY	EFFORT	ISO GAPS REMEDIATED	REMEDIATION TIME
MEDIUM	HIGH	12	3 months

Deploy a centralized logging server that will capture all logs and alerts that are created by servers and systems.

#	Activity	Resource	Effort
1	Deploy a centralized logging server that will aggregate logs from all information systems (networking devices, workstations, servers, etc.). The logging server can be the in-house Splunk or one that can be shared with Logistec. Ideally you would want all logs fed into one system. The system would then correlate events and alert if specified criteria is met. The alerts must detect if logs are tampered with or unauthorized access occurs.	● Information Security	12 weeks

3.4.4 Logical Access Control Improvement

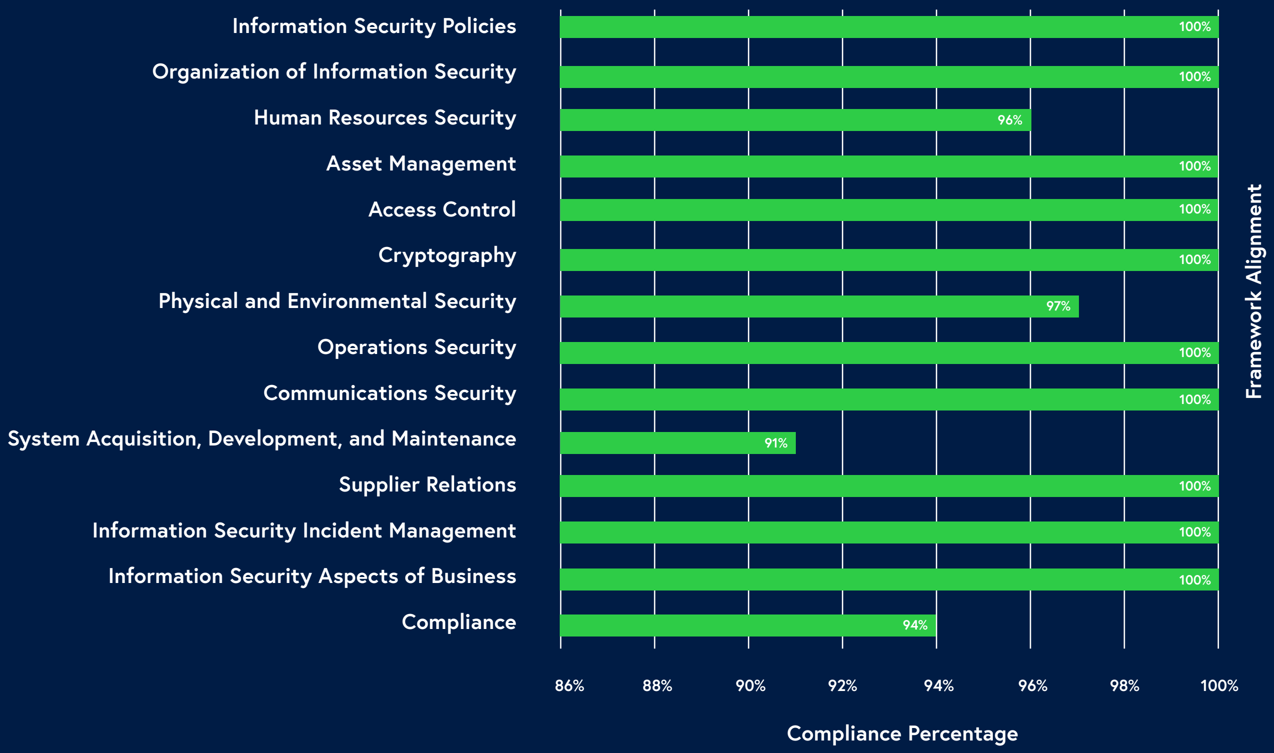
PRIORITY	EFFORT	ISO GAPS REMEDIATED	REMEDIATION TIME
MEDIUM	MEDIUM	9, 11, 13	5 months

Develop and refine logical access controls to secure the network. Doing so will prevent individuals from gaining access to the restricted internal network.

#	Activity	Resource	Effort
1	Segment networks with firewall rules where production, testing and operations are separated. Segments not needing access to the sensitive zones should be restricted.	• Information Security	4 weeks
2	Refine existing network security controls by implementing restrictions on which devices can join the network when directly plugged in (Network Access Control (NAC)).	• Information Security	4 weeks
3	Administrative accounts should be divided into different tiers where each account serves an individual purpose. Doing so will prevent attackers from pivoting.	• Information Technology • Information Security	4 weeks
4	Enable two-factor authentication on all services that support it (e.g., email and VPN)	• Information Technology • Information Security	4 weeks
5	Review currently security control configurations for areas of improvement. This should include all existing security controls (e.g., can Sophos have additional changes to catch suspicious events better)	• Information Security	4 weeks

4. Post Remediation Compliance

Upon completion of the roadmap, ACME Inc.'s framework score for all ISO/EIC 27001 domains would be **98%**. A full 100% would require additional specifics that we deemed not worth the additional effort given the vast amount of work already required.



Ready to strengthen your security posture?

There's simply no room for compromise.

Get in touch to share your cybersecurity needs with our team and get a free quote.

☎ 647 797 9230 @ info@packetlabs.net packetlabs.net

606-6733 Mississauga Road, Mississauga, ON, L5N 6J5

@pktlabs /packetlabs-ltd- @packetlabs

Scan QR code to book a virtual consultation with us.

Packetlabs