ISO 27001 Report - Apex

Your Organisation Name

June 29, 2020

Prepared By:
Admin Account

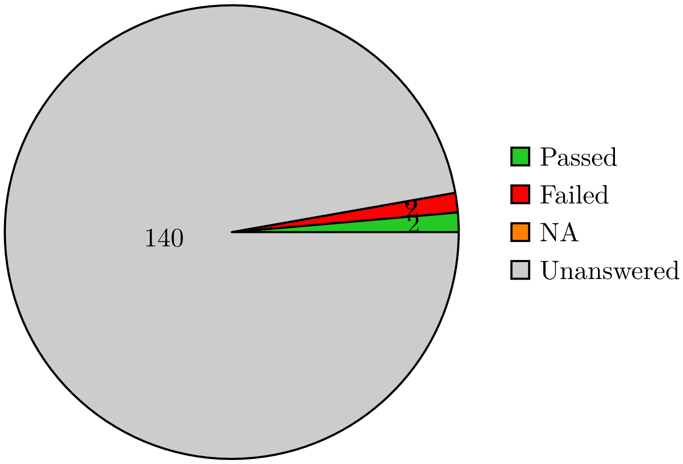
Contents

1 Executive Summary

50

Assessment Score

None



2 Results Overview

Module	Incl in Assessment	# Areas Covered	Pass %	Failure %	Not Applicable
A.5 Security policy	Yes	3	100%	0%	0
A.6 Organization of information security	Yes	12	83%	17%	0
A.7 Asset management	Yes	6	100%	0%	0
A.8 Human resources security	Yes	10	100%	0%	0
A.9 Physical and environmental security	Yes	14	100%	0%	0
A.10 Communications and operations management	Yes	33	100%	0%	0
A.11 Access control	Yes	26	100%	0%	0
A.12 Information systems acquisition, development and maintenance	Yes	17	100%	0%	0
A.13 Information security incident management	Yes	6	100%	0%	0
A.14 Business continuity management	Yes	6	100%	0%	0
A.15 Compliance	Yes	11	100%	0%	0

3 Action Plan Summary

Module	Question	Action Plan	Priority	Due Date	Status
A.6.1 Internal organization	A.6.1.1 Management commitment to information secur..		Medium	None	Overdue
A.6.1 Internal organization	A.6.1.2 Information security coordination		Medium	None	Overdue

4 Identified Risks with Action Plan

These are risks that have been identified, evaluated, and have an Action Plan. We have identified 0 high, 2 medium, and 0 low action items. Of all items in the action plan, 2 are pending and 0 are complete.

4.1 A.6.1.1 Management commitment to information security

Module: A.6.1 Internal organization

Response: Partially Implemented

Comments: This control is partially implemented according to the description and intent of the control. Required evidence, if any, is attached.

Action Plan: None

Status: Overdue

Priority: Medium

Target Date for Completion: None

4.2 A.6.1.2 Information security coordination

Module: A.6.1 Internal organization

Response: Not Implemented

Comments: This control is not implemented yet according to the description and intent of the control. Required evidence, if any, is attached.

Action Plan: None

Status: Overdue

Priority: Medium

Target Date for Completion: None

5 Managed or Not Present Risks

Problems that have been managed or are not present in your organization.

5.1 A.5 Security policy

5.1.1 A.5.1 Information security policy

5.1.1.1 A.5.1.1 Information security policy document

Response: Implemented

Comments: This control is fully implemented according to the description and intent of the control. Required evidence, if any, is attached.

5.1.1.2 A.5.1.2 Review of the information security policy

Response: Implemented

Comments: This control is fully implemented according to the description and intent of the control. Required evidence, if any, is attached.

6 Unidentified Risks

Risks that have not been identified yet due to question not being answered.

6.1 A.6 Organization of information security

6.1.1 Overview of "ORGANIZATION OF INFORMATION SECURITY" policy

6.1.2 A.6.1 Internal organization

6.1.2.1 A.6.1.3 Allocation of information security responsibilities

6.1.2.2 A.6.1.4 Authorization process for information processing facilities

6.1.2.3 A.6.1.5 Confidentiality agreements

6.1.2.4 A.6.1.6 Contact with authorities

6.1.2.5 A.6.1.7 Contact with special interest groups

6.1.2.6 A.6.1.8 Independent review of information security

6.1.3 A.6.2 External parties

6.1.3.1 A.6.2.1 Identification of risks related to external parties

6.1.3.2 A.6.2.2 Addressing security when dealing with customers

6.1.3.3 A.6.2.3 Addressing security in third party agreements

6.2 A.7 Asset management

6.2.1 Overview of "ASSET MANAGEMENT" policy

6.2.2 A.7.1 Responsibility for assets

6.2.2.1 A.7.1.1 Inventory of assets

6.2.2.2 A.7.1.2 Ownership of assets

6.2.2.3 A.7.1.3 Acceptable use of assets

6.2.3 A.7.2 Information classification

6.2.3.1 A.7.2.1 Classification guidelines

6.2.3.2 A.7.2.2 Information labelling and handling

6.3 A.8 Human resources security

6.3.1 Overview of "HUMAN RESOURCES SECURITY" policy

6.3.2 A.8.1 Prior to employment 4)

6.3.2.1 A.8.1.1 Roles and responsibilities

6.3.2.2 A.8.1.2 Screening

6.3.2.3 A.8.1.3 Terms and conditions of employment

6.3.3 A.8.2 During employment

6.3.3.1 A.8.2.1 Management responsibilities

6.3.3.2 A.8.2.2 Information security awareness, education and training

6.3.3.3 A.8.2.3 Disciplinary process

6.3.4 A.8.3 Termination or change of employment

6.3.4.1 A.8.3.1 Termination responsibilities

6.3.4.2 A.8.3.2 Return of assets

6.3.4.3 A.8.3.3 Removal of access rights

6.4 A.9 Physical and environmental security

6.4.1 Overview of "PHYSICAL AND ENVIRONMENTAL SECURITY" policy

6.4.2 A.9.1 Secure areas

6.4.2.1 A.9.1.1 Physical security perimeter

6.4.2.2 A.9.1.2 Physical entry controls

6.4.2.3 A.9.1.3 Securing offices, rooms and facilities

6.4.2.4 A.9.1.4 Protecting against external and environmental threats

6.4.2.5 A.9.1.5 Working in secure areas

6.4.2.6 A.9.1.6 Public access, delivery and loading areas

6.4.3 A.9.2 Equipment security

6.4.3.1 A.9.2.1 Equipment siting and protection

6.4.3.2 A.9.2.2 Supporting utilities

6.4.3.3 A.9.2.3 Cabling security

6.4.3.4 A.9.2.4 Equipment maintenance

6.4.3.5 A.9.2.5 Security of equipment off premises

6.4.3.6 A.9.2.6 Secure disposal or re-use of equipment

6.4.3.7 A.9.2.7 Removal of property

6.5 A.10 Communications and operations management

6.5.1 Overview of "COMMUNICATIONS AND OPERATIONS MANAGEMENT" policy

6.5.2 A.10.1 Operational procedures and responsibilities

6.5.2.1 A.10.1.1 Documented operating procedures

6.5.2.2 A.10.1.2 Change management

6.5.2.3 A.10.1.3 Segregation of duties

6.5.2.4 A.10.1.4 Separation of development, test and operational facilities

6.5.3 A.10.2 Third party service delivery management

6.5.3.1 A.10.2.1 Service delivery

6.5.3.2 A.10.2.2 Monitoring and review of third party services

6.5.3.3 A.10.2.3 Managing changes to third party services

6.5.4 A.10.3 System planning and acceptance

6.5.4.1 A.10.3.1 Capacity management

6.5.4.2 A.10.3.2 System acceptance

6.5.5 A.10.4 Protection against malicious and mobile code

6.5.5.1 A.10.4.1 Controls against malicious code

6.5.5.2 A.10.4.2 Controls against mobile code

6.5.6 A.10.5 Back-up

6.5.6.1 A.10.5.1 Information back-up

6.5.7 A.10.6 Network security management

6.5.7.1 A.10.6.1 Network controls

6.5.7.2 A.10.6.2 Security of network services

6.5.8 A.10.7 Media handling

6.5.8.1 A.10.7.1 Management of removable media

6.5.8.2 A.10.7.2 Disposal of media

6.5.8.3 A.10.7.3 Information handling procedures

6.5.8.4 A.10.7.4 Security of system documentation

6.5.9 A.10.8 Exchange of information

6.5.9.1 A.10.8.1 Information exchange policies and procedures

6.5.9.2 A.10.8.2 Exchange agreements

6.5.9.3 A.10.8.3 Physical media in transit

6.5.9.4 A.10.8.4 Electronic messaging

6.5.9.5 A.10.8.5 Business information systems

6.5.10 A.10.9 Electronic commerce services

6.5.10.1 A.10.9.1 Electronic commerce

6.5.10.2 A.10.9.2 On-line transactions

6.5.10.3 A.10.9.3 Publicly available information

6.5.11 A.10.10 Monitoring

6.5.11.1 A.10.10.1 Audit logging

6.5.11.2 A.10.10.2 Monitoring system use

6.5.11.3 A.10.10.3 Protection of log information

6.5.11.4 A.10.10.4 Administrator and operator logs

6.5.11.5 A.10.10.5 Fault logging

6.5.11.6 A.10.10.6 Clock synchronization

6.6 A.11 Access control

6.6.1 Overview of "ACCESS CONTROL" Policy

6.6.2 A.11.1 Business requirement for access control

6.6.2.1 A.11.1.1 Access control policy

6.6.3 A.11.2 User access management

6.6.3.1 A.11.2.1 User registration

6.6.3.2 A.11.2.2 Privilege management

6.6.3.3 A.11.2.3 User password management

6.6.3.4 A.11.2.4 Review of user access rights

6.6.4 A.11.3 User responsibilities

6.6.4.1 A.11.3.1 Password use

6.6.4.2 A.11.3.2 Unattended user equipment

6.6.4.3 A.11.3.3 Clear desk and clear screen policy

6.6.5 A.11.4 Network access control

6.6.5.1 A.11.4.1 Policy on use of network services

6.6.5.2 A.11.4.2 User authentication for external connections

6.6.5.3 A.11.4.3 Equipment identification in networks

6.6.5.4 A.11.4.4 Remote diagnostic and configuration port protection

6.6.5.5 A.11.4.5 Segregation in networks

6.6.5.6 A.11.4.6 Network connection control

6.6.5.7 A.11.4.7 Network routing control

6.6.6 A.11.5 Operating system access control

6.6.6.1 A.11.5.1 Secure log-on procedures

6.6.6.2 A.11.5.2 User identification and authentication

6.6.6.3 A.11.5.3 Password management system

6.6.6.4 A.11.5.4 Use of system utilities

6.6.6.5 A.11.5.5 Session time-out

6.6.6.6 A.11.5.6 Limitation of connection time

6.6.7 A.11.6 Application and information access control

6.6.7.1 A.11.6.1 Information access restriction

6.6.7.2 A.11.6.2 Sensitive system isolation

6.6.8 A.11.7 Mobile computing and teleworking

6.6.8.1 A.11.7.1 Mobile computing and communications

6.6.8.2 A.11.7.2 Teleworking

6.7 A.12 Information systems acquisition, development and maintenance

6.7.1 Overview of "INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE" policy

6.7.2 A.12.1 Security requirements of information systems

6.7.2.1 A.12.1.1 Security requirements analysis and specification

6.7.3 A.12.2 Correct processing in applications

6.7.3.1 A.12.2.1 Input data validation

6.7.3.2 A.12.2.2 Control of internal processing

6.7.3.3 A.12.2.3 Message integrity

6.7.3.4 A.12.2.4 Output data validation

6.7.4 A.12.3 Cryptographic controls

6.7.4.1 A.12.3.1 Policy on the use of cryptographic controls

6.7.4.2 A.12.3.2 Key management

6.7.5 A.12.4 Security of system files

6.7.5.1 A.12.4.1 Control of operational software

6.7.5.2 A.12.4.2 Protection of system test data

6.7.5.3 A.12.4.3 Access control to program source code

6.7.6 A.12.5 Security in development and support processes

6.7.6.1 A.12.5.1 Change control procedures

6.7.6.2 A.12.5.2 Technical review of applications after operating system changes

6.7.6.3 A.12.5.3 Restrictions on changes to software packages

6.7.6.4 A.12.5.4 Information leakage

6.7.6.5 A.12.5.5 Outsourced software development

6.7.7 A.12.6 Technical Vulnerability Management

6.7.7.1 A.12.6.1 Control of technical vulnerabilities

6.8 A.13 Information security incident management

6.8.1 Overview of "INFORMATION SECURITY INCIDENT MANAGEMENT" policy

6.8.2 A.13.1 Reporting information security events and weaknesses

6.8.2.1 A.13.1.1 Reporting information security events

6.8.2.2 A.13.1.2 Reporting security weaknesses

6.8.3 A.13.2 Management of information security incidents and improvements

6.8.3.1 A.13.2.1 Responsibilities and procedures

6.8.3.2 A.13.2.2 Learning from information security incidents

6.8.3.3 A.13.2.3 Collection of evidence

6.9 A.14 Business continuity management

6.9.1 Overview of "BUSINESS CONTINUITY MANAGEMENT" policy

6.9.2 A.14.1 Information security aspects of business continuity management

6.9.2.1 A.14.1.1 Including information security in the business continuity management process

6.9.2.2 A.14.1.2 Business continuity and risk assessment

6.9.2.3 A.14.1.3 Developing and implementing continuity plans including information security

6.9.2.4 A.14.1.4 Business continuity planning framework

6.9.2.5 A.14.1.5 Testing, maintaining and reassessing business continuity plans

6.10 A.15 Compliance

6.10.1 Overview of "COMPLIANCE" policy

6.10.2 A.15.1 Compliance with legal requirements

6.10.2.1 A.15.1.1 Identification of applicable legislation

6.10.2.2 A.15.1.2 Intellectual property rights (IPR)

6.10.2.3 A.15.1.3 Protection of organizational records

6.10.2.4 A.15.1.4 Data protection and privacy of personal information

6.10.2.5 A.15.1.5 Prevention of misuse of information processing facilities

6.10.2.6 A.15.1.6 Regulation of cryptographic controls

6.10.3 A.15.2 Compliance with security policies and standards, and technical compliance

6.10.3.1 A.15.2.1 Compliance with security policies and standards

6.10.3.2 A.15.2.2 Technical compliance checking

6.10.4 A.15.3 Information systems audit considerations

6.10.4.1 A.15.3.1 Information systems audit controls

6.10.4.2 A.15.3.2 Protection of information systems audit tools

6.11 A.5 Security policy

6.11.1 Overview of "SECURITY" policy

DISCLAIMER - Information provided by Your Organisation Name for this assessment was not independently verified by Databrackets; Your Organisation Name has provided details about their operation to the best of their knowledge. These reports and recommendations are for evaluation purposes only and not intended to be construed as legal advice. Your Organisation Name is advised to consult with attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on the company and/or its personnel.