UnderDefense
CYBERSECURITY

ISO 27001 Initial Assessment Report

[Anonymized]

Please be informed that this is an incomplete version of the ISO 27001 Initial Assessment Report

Get full report

Table of contents

Executive Summary

[CLIENT] has requested that UnderDefense, as an independent and trusted Cyber Security partner, conducts an assessment and analysis of the current state of the information security program of the organization and its compliance with ISO 27001:2013 standard. ISO 27001 (ISO 27001:2013) is an international standard for the implementation of a best practice Information Security Management System (ISMS). ISO 27001 accreditation requires an organisation to bring information security under explicit management control.

The objective of the assessment was to document the current state of the ISMS and Annex A controls at [CLIENT] sites, understand the state, and recommend actions needed to achieve the required state to prepare for ISO/IEC 27001 certification.

Our methodology

[CLIENT] has requested that UnderDefense, as an independent and trusted Cyber Security partner, conducts an assessment and analysis of the current state of the information security program of the organization and its compliance with ISO 27001:2013 standard. ISO 27001 (ISO 27001:2013) is an international standard for the implementation of a best practice Information Security Management System (ISMS). ISO 27001 accreditation requires an organisation to bring information security under explicit management control.

The objective of the assessment was to document the current state of the ISMS and Annex A controls at [CLIENT] sites, understand the state, and recommend actions needed to achieve the required state to prepare for ISO/IEC 27001 certification.

Key stakeholders interviewed

The first important step of our assessment was the interview with the key stakeholders and employees to collect information and check on practice the current control set and the risks that knowledge keepers observe in the organization. The following table represents a list of individuals who took part in the interview. The respondents shared the information regarding information security in their organization, presented current controls of information security in their departments and answered questions from ISO 27001 checklists regarding processes, finance, systems, infrastructure, business processes, policies, growth plans, endpoint security, operating systems, access controls, valuable assets, risks, etc.

Position in the company	Respondent
Director of Operations	
IT Director	
Head of CIS (corp. information systems)	
Managing Director	
HR Department	
Accounting Department	
HR Director	
DevOps	
PMO Director	
QA Director	
Head of Recruiting	

Maturity Level for each clause of ISO 27001

To illustrate the conformity to ISO 27001, we have assigned a level of coverage based upon the legend below.

UD Observation Ranking (Conforms or Major and Minor non-conformity)(Conformity Rating)	Description
Major	Significant improvement needed (major non-conformities and/or significant number of minor non-conformities)
Minor	Minor to moderate improvement needed (minor non-conformities and/or observations)
Conforms	Certification ready
Observation	Informational comment not impacting certification readiness
Cannot be assessed	The control cannot be assessed as it has not been neither designed or implemented and it's applicability to [CLIENT] ISMS is not defined

None of these shortfalls are insurmountable, but addressing them will require management commitment to establish, implement, maintain and improve a comprehensive ISMS.

Conclusions

Radar chart below provides a graphical summary of the assessment outcome. The chart describes the current maturity level of each ISO/IEC 27001:2013 Annex A control. Each maturity level corresponds to numeric level on the chart:

- Level 1 - Major non-conformity,
- Level 2 - Minor non-conformity,
- Level 3 - Conforms

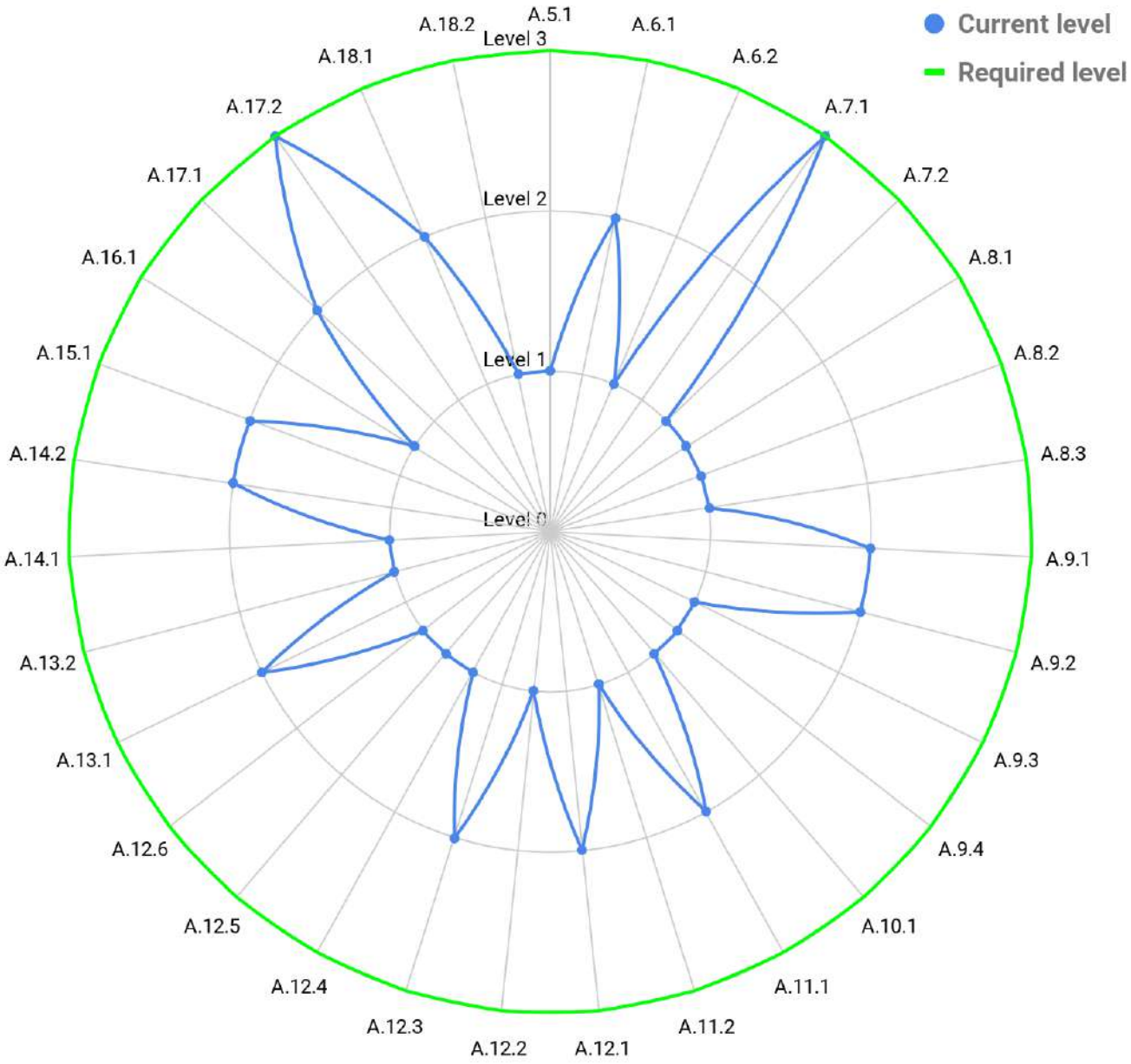

Figure 1. Graphical representation of each maturity level.

RoadMap

[CLIENT] needs to assign roles and responsibilities, to handle all actions related to the analysis of the non-conformity, execution of improvements and controls implementation to achieve the acceptable state for certification.

The table below shows ISO 27001:2013 controls ordered and prioritized by severity of Maturity Levels.

The table represents step by step guide to start executing improvements on minor non-conformity clauses and proceed with major non-conformity. It is highly recommended to follow the order, controls, which marked as Conforms, represent what's already in place and working well, minor non-conformities can be resolved by one-time activities(e.g. waterfall methodology), major non-conformities requires iterative, team-based approach, in order complete all activities, resolve issues effectively and in time.

The table can be treated as a project plan that contents 3 Stages, as presented in the table below, which represent required steps for successful transition and compliance.

	Control	Respondent
	Recommendations - Appendix A	
	A.7.1 Prior to employment	Conforms
	A.17.2 Redundancies	Conforms
1	**Stage 1**	
1.1	A.6.1 Internal Organisation	Minor non-conformity
1.2	A.9.1 Business requirements for access control	Minor non-conformity
1.3	A.9.2 User access management	Minor non-conformity
1.4	A.11.1 Secure areas	Minor non-conformity
1.5	A.12.1 Operational procedures and responsibilities	Minor non-conformity
1.6	A.12.3 Backup	Minor non-conformity
1.7	A.13.1 Network security management	Minor non-conformity
1.8	A.14.2 Security in development and support processes	Minor non-conformity
1.9	A.15.1 Information security in supplier relationships	Minor non-conformity
1.10	A.17.1 Information security continuity	Minor non-conformity
1.11	A.18.1 Compliance with legal and contractual requirements	Minor non-conformity

	Control	Respondent
2	**Stage 2**	
2.1	A.6.2 Mobile devices and teleworking	Major non-conformity
2.2	A.7.2 During employment	Major non-conformity
2.3	A.8.1 Responsibility for assets	Major non-conformity
2.4	A.8.2 Information Classification	Major non-conformity
2.5	A.8.3 Media handling	Major non-conformity
2.6	A.9.3 User responsibilities	Major non-conformity
2.7	A.9.4 System and application access control	Major non-conformity
2.8	A.10.1 Cryptographic controls	Major non-conformity
2.9	A.11.2 Equipment	Major non-conformity
2.10	A.12.2 Protection from malware	Major non-conformity
2.11	A.12.4 Control of operational software	Major non-conformity
2.12	A.12.5 Controls against malware	Major non-conformity
2.13	A.12.6 Technical vulnerability management	Major non-conformity
2.14	A.13.2 Information transfer	Major non-conformity
2.15	A.14.1 Security requirements of information systems	Major non-conformity
2.16	A.16.1 Management of information security incidents and improvements	Major non-conformity
2.17	A.18.2 Information security reviews	Major non-conformity
2.18	A.5.1 Management direction for information security	Major non-conformity
	Cannot be assessed	
	A.12.7 Information systems audit considerations	Cannot be assessed
	A.14.3 Test data	Cannot be assessed
	A.15.2 Supplier service delivery management	Cannot be assessed
	Recommendations – ISMS activities	
3	**Stage 3**	
3.1	Stage 3Scope Definition	Major non-conformity
3.2	A.15.2 Supplier service delivery management	Major non-conformity
3.2	A.15.2 Supplier service delivery management	Major non-conformity
3.3	Treatment of Risks, including Statement of Applicability	Major non-conformity
3.3	Treatment of Risks, including Statement of Applicability	Major non-conformity

	Control	Respondent
3.4	Risk Treatment Plan	Major non-conformity
3.5	Monitoring, Review of the ISMS & Effectiveness of Controls	Major non-conformity
3.6	ISMS Improvement including Corrective & Preventive Actions	Major non-conformity

Recommendations – ISMS activities

The tables on the subsequent pages include recommendations for improvements needed to achieve the level of maturity required for ISO 27001 certification (Required target state).

The actions are divided into the Plan, Do, Check and Act phases of the [CLIENT]'s Information Security Management System (ISMS). The Plan-Do-Check-Act (PDCA) cycle is an iterative process and with each iteration the organization has the opportunity to (re-)define the scope of its Information Security Management System, (re-)define risks, (re-)select controls and adjust or create processes, policies and guidelines.

All activities listed within this section must be completed in advance of the initial certification audit.

Note, each stage of the PDCA cycle requires approach documents to be created (i.e. policy/ procedure documents). It is up to the discretion of management to determine if these documents should be created during the Plan stage or if they should be developed during the respective stages in which the documents will be used.

These recommendations represent typical activities needed to implement and operate an ISMS and to prepare for ISO 27001 certification. [CLIENT] management will need to ultimately decide what actions to undertake within their environment.

Check stageN/A

Monitoring, Review of the ISMS & Effectiveness of Controls	
Short description	The ISMS should be monitored to detect and act on errors and security incidents. Regular reviews on the effectiveness of the ISMS, the relevant controls and the Risk Assessment should be performed
UD Observations	The organization has not developed a document which describes the activities that should be taken at each stage of ISMS implementation, including “Check” stage.
UD Observation Ranking	Major non-conformity
Recommendations	• Monitor and review procedures that are executed to detect and act on errors and security incidents. • Execute a security managers meeting in which all security related developments are discussed (e.g. errors and security incidents). Review the ISMS Policy and objectives, measure the effectiveness of controls and the Risk Assessment process.
Documents reviewed	• N/A