Case Study

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

ISO 27001:2013 Initial Assessment

Compliance

Solution/Service Title	ISO/IEC 27001:2013 Initial Assessment
Client Industry	Cloud based CRM implementation services and Mobile applications to industries such as Pharmatech, Healthcare, and Finance
Client Overview	International Software and Technology Services company
Client Challenge	Preparation to ISO 27001:2013 Certification, development and implementation of a rigorous security program, which includes the development and implementation of an Information Security Management System (ISMS)
Scope	The scope of this assessment is bounded by specified services of company and specified facilities. The in-scope applications, systems, people, and processes are globally implemented, operated by teams and are specifically defined in the scope and bounds.
Key Benefits	UnderDefense reviewed compliance of all documents, records and procedures with certification point of view. Identified non conformance with respective certification process and documentation and assisted the organization in preparing for final certification.
Results	The team prepared comprehensive roadmap to rapidly eliminate nonconformities, detailed recommendations following the ISO/IEC 27002:2013 best practice guidance. These controls include but are not limited to: Incident Response, Antivirus Controls, Vulnerability Management, Security Awareness, Remote Work Controls, etc.

Certifications

Ph.D. in Security

Big Picture of the Certification Journey

Stage 1

This initial assessment determines if the mandatory requirements of the standard are being met and if the management system is capable of proceeding to stage 2.

Stage 2

This second assessment determines the effectiveness of the system, and seeks to confirm that the management system is implemented and operational.

Recommendation for Certification

At this point in the process we review any correctve actions taken to address findings raised at Stage 1 & 2. Certification may be recommended.

Certification Review & Decision

The organisation's files are reviewed by an independent and impartial panel and the certification decision is made.

Certification Achieved

Successful certification is communicated to the client. Certificates are issued.

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

ISO/IEC 27001:2013 Annex A Reference

Annex A is a link to ISO/IEC 27002 - a code of practice, a generic, advisory document, not a formal specification such as ISO/IEC 27001. It recommends information security controls addressing information security control objectives arising from risks to the confidentiality, integrity and availability of information.
There are 14 clauses containing 35 control categories which are divided into 114 controls.

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

Team composition

1 ISO 27001 Lead Auditor
2 Cyber Security Auditors

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

Initial Assessment Overview

1 Documentation analysis

Informal review of the ISMS, for example checking the existence and completeness of key documentation such as the organization's information security policy, Statement of Applicability (SoA) and Risk Treatment Plan (RTP). This stage serves to familiarize the assessors with the organization and vice versa.

2 Interviews phase

A more detailed and formal check, independently testing the ISMS against the requirements specified in ISO/IEC 27001. The assessors will seek evidence to confirm that the management system has been properly designed and implemented, and is in fact in operation (for example by confirming that a security committee or similar management body meets regularly to oversee the ISMS).

3 Security posture analysis

UD team process findings collected during interviews and checks, this is the phase where we write down what we have found during the main audit – names of persons we spoke to, quotes of what respondent said, IDs and content of records we examined, description of facilities we visited, observations about the equipment we checked, etc

4 Recommendations

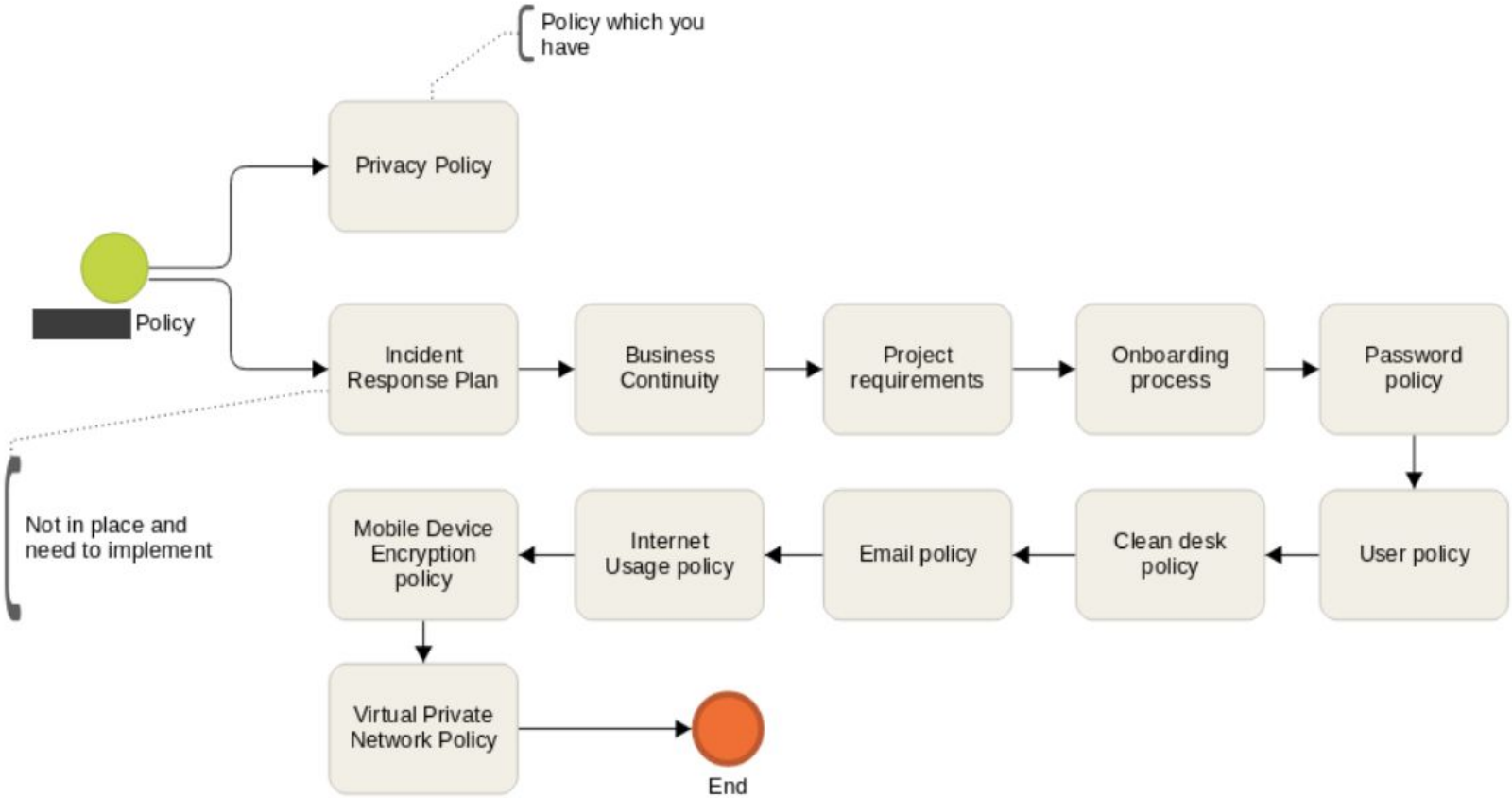
Following the evaluation, the team prepare comprehensive roadmap to rapidly eliminate nonconformities, detailed recommendations following the ISO/IEC 27002:2013 best practice guidance

5 Final results

The team deliver Initial Assessment Report, make final presentation that represent key findings and mapped roadmap to future improvements

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

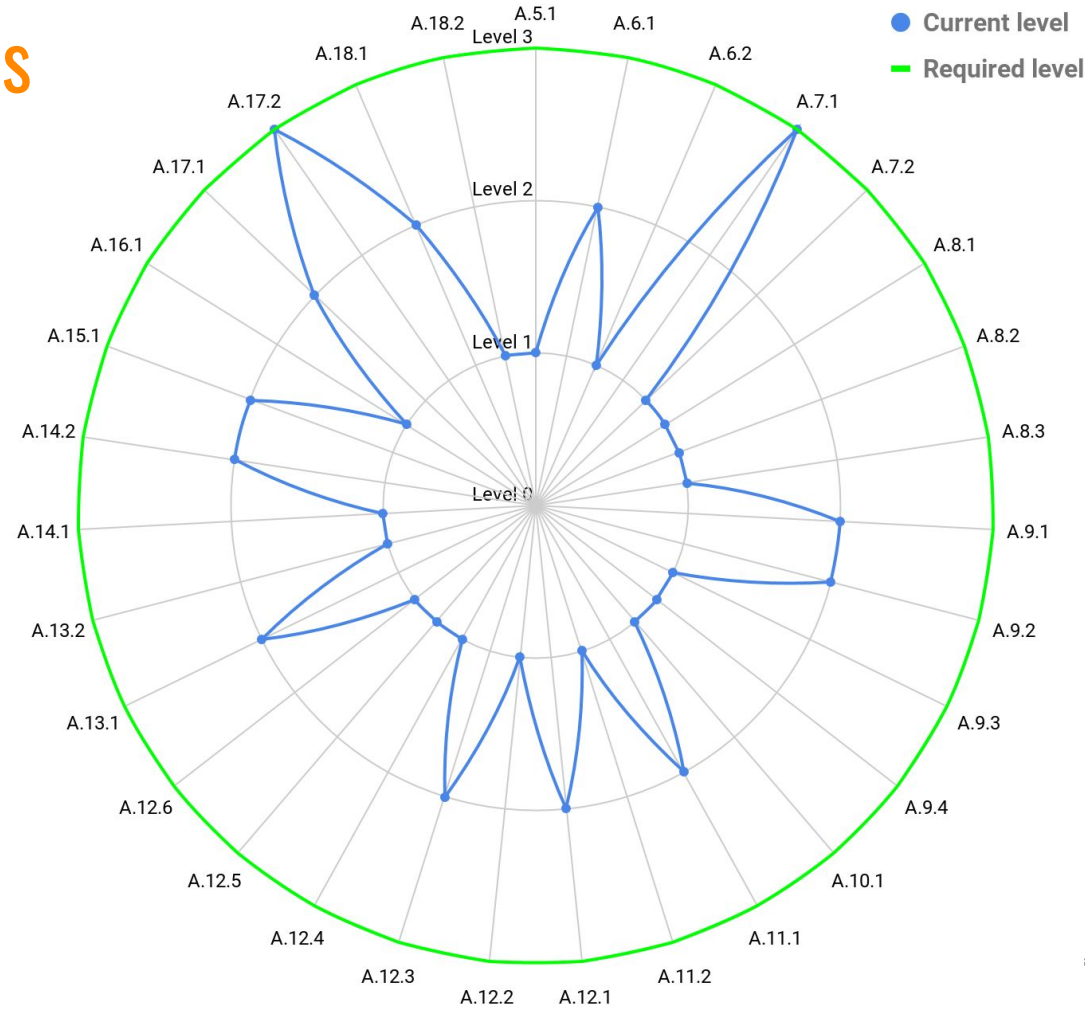
Documentation analysis



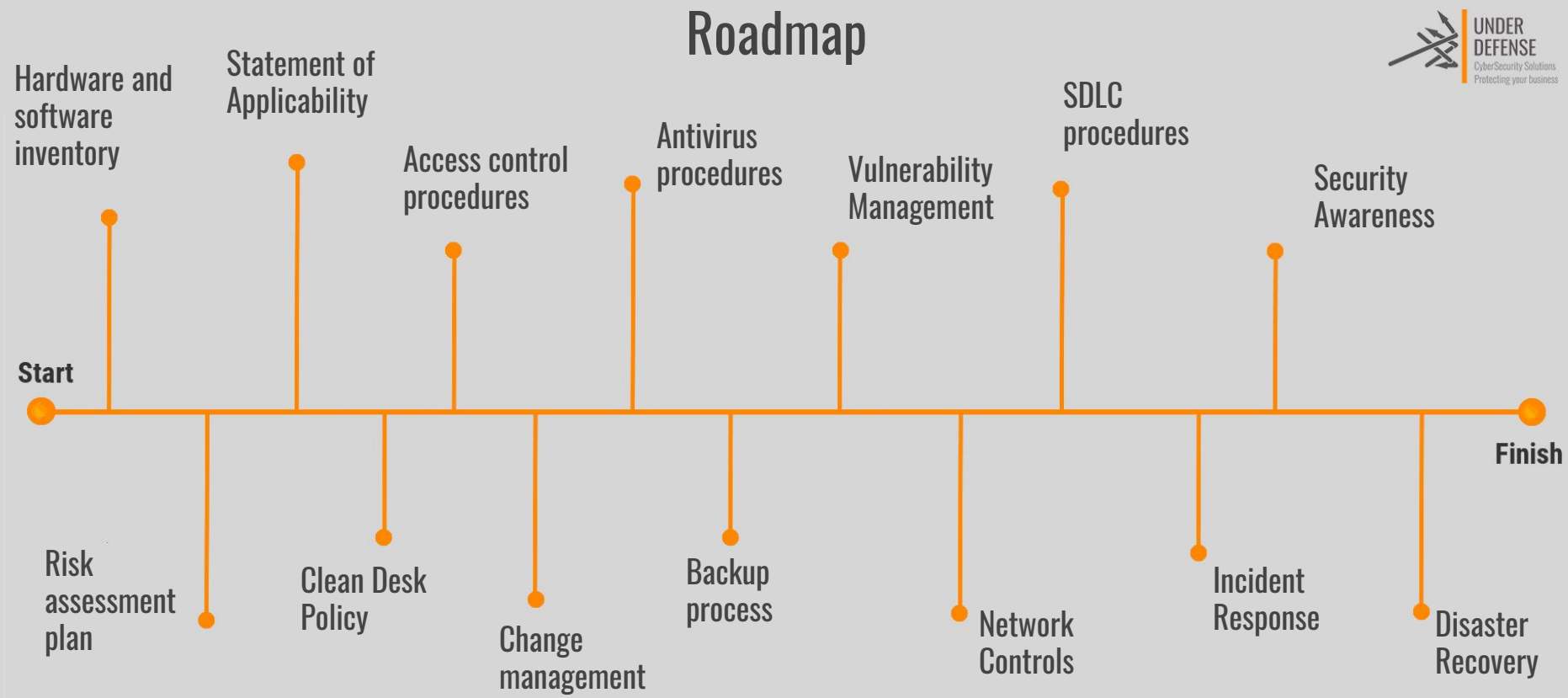
Security posture analysis

Radar chart 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



Recommendations



Final results

UnderDefense provide reports with detailed information on identified gaps, their criticality and recommendation for improvement. Review key findings and results during a facilitated discussion. As outcome of assessment project we deliver aligned with client, clearly defined and approved security strategy that will help organization to achieve its business goals and meet security compliance and best practices.

A.12.6 Technical vulnerability management	
Short description	To prevent exploitation of technical vulnerabilities.
ISO 27001 Control	A.12.6.1 Management of technical vulnerabilities A.12.6.2 Restrictions on software installation
UnderDefense Observations	• Windows Server Update Services (WSUS) is deployed as a patch management tool. • Control procedures for vulnerabilities management is not performed for Unix based server and user software. • Vulnerability scan represented only as a network security scan. It states that the vulnerability scan (network security scan) should be performed once a month. • The organization has not implemented policy which defines roles, responsibilities, timelines and procedures within vulnerability management process.
UnderDefense Observation Ranking	Major non-conformity
Recommendations	• Document and implement separate Vulnerability Management Policy establishes procedures for identifying and promptly remediating vulnerabilities to minimize security breaches associated with unpatched vulnerabilities. Establish and document guidelines for software installation which make users aware of what organization deems as acceptable and unacceptable software that is installed (e.g. whitelists)
Documents reviewed	SOP501_Logical_and_Physical_Security.pdf

Thank you!

Call us now at +1 929 999 5101