UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

ISO 27001 Initial Assessment Report

for [CLIENT]

September 2018

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

Our methodology is based on the interview and practical evaluation with the key stakeholders, reviewing technical documentation and checking readiness to conduct ISO/IEC 27001 certification. All the findings are mapped on ISO/IEC 27001:2013 standard (see below). Rating provided in form of Maturity Level matrix and Radar chart.

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

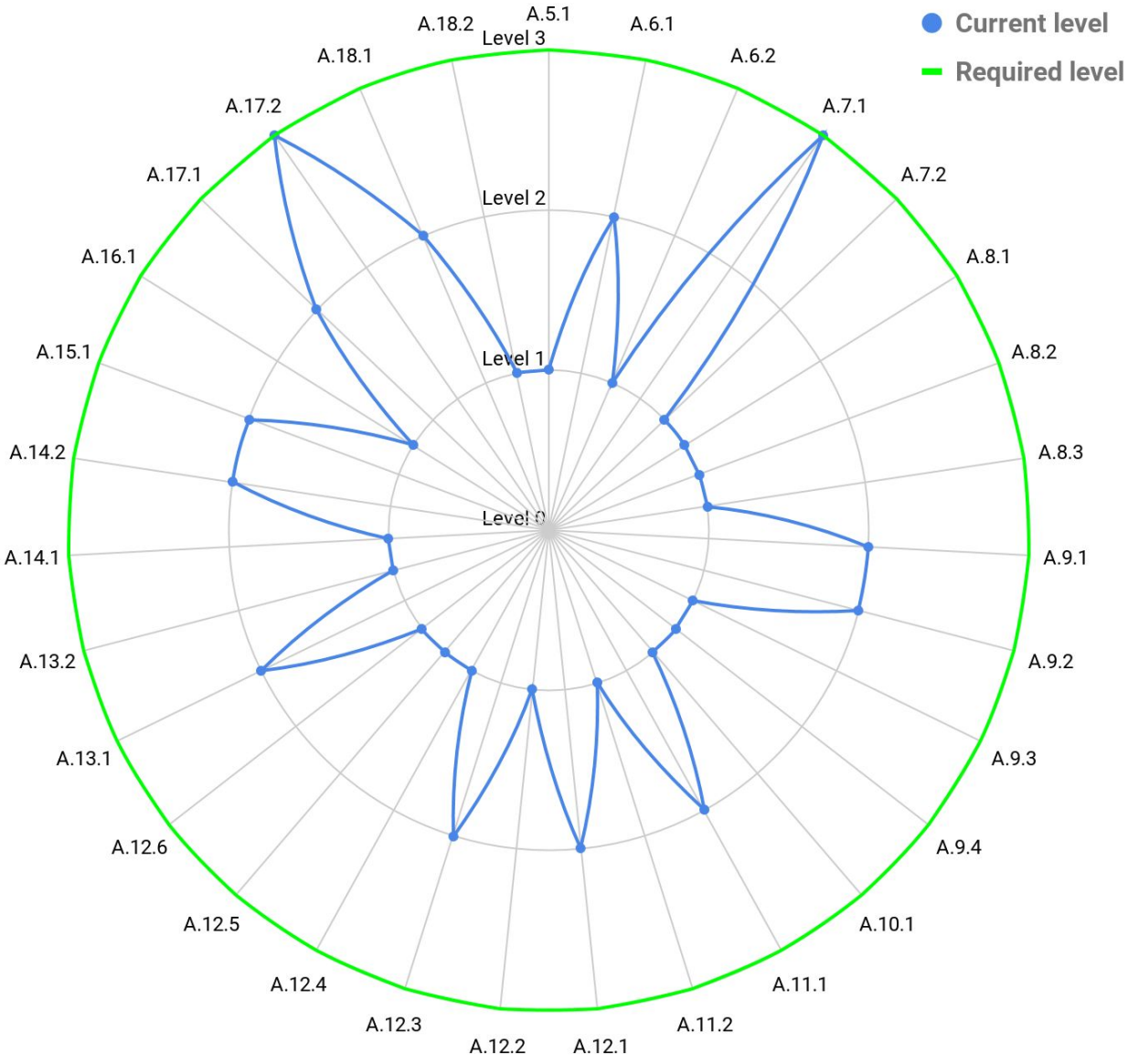

Figure 1. Graphical representation of each maturity level.

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	Maturity Level
	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**
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	Scope Definition	**Major non-conformity**
3.2	Risk Assessment Approach and Execution	**Major non-conformity**
3.3	Treatment of Risks, including Statement of Applicability	**Major non-conformity**
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.

Plan stage

Scope Definition	
Short description	The ISMS scope should be defined in terms of characteristics of the business, the organization, its locations, assets and technologies.
UD Observations	● ISMS scope is not documented and approved by management. The scope contains the list of the areas, locations, assets, and technologies of the organization controlled by the ISMS. Exclusions from the scope are not documented and justified.
UD Observation Ranking	● Major non-conformity
Recommendations	● Document ISMS scope including the list of the areas, locations, assets, and technologies of the organization. ● Document all exclusions from ISMS scope (e.g., sales representative offices, software developed by client-facing project teams, etc.), and justification for exclusion from scope. ● Review and re-approve ISMS scope document with management annually or in cases if significant changes to the environment occur outside of the annual review cycle (e.g. regulatory changes, inclusion of new locations, etc.).
Documents reviewed	N/a

Risk Assessment Approach and Execution	
Short description	A Risk Assessment approach should be created for the organization.
UD Observations	● The organization has not developed and documented a comprehensive Risk Management Framework that describes all steps and relevant methods required to be carried out in terms of risk assessment process, including: - Asset Identification - Threat Identification - Vulnerability Identification - Control Analysis - Likelihood Determination - Impact Analysis - Risk Determination - Control Recommendations - Results Documentation ● The organization has not defined and documented the lists of assets that are included within ISMS scope.

UD Observation Ranking	Major non-conformity
Recommendations	• Create Risk Management Framework document contains risk levels matrix which is based on a 5-level scale (Very Low to Very High), and provides the instructions for risk level determination. • Adjust Risk Assessment Framework so that it includes the criteria for accepting risk and identifying the acceptable level of (e.g. at what level can risk automatically be accepted and under what circumstances). Approval should be obtained from high-level management for the decision to accept residual risks, and authorization obtained for the actual operation of the ISMS. • Review the documents containing the lists of assets and define a single comprehensive list of assets along with asset owners while considering above mentioned recommendation.
Documents reviewed	N/a

Treatment of Risks, including Statement of Applicability	
Short description	Select the method for treating risks identified and obtain management approval for the proposed residual risks.
UD Observations	• A Statement of Applicability (SOA) document is not available at [CLIENT]. • For the external certification Statement of Applicability is a key evidence of the steps taken between risk assessment and implementation of appropriate controls.
UD Observation Ranking	Major non-conformity
Recommendations	• The SOA document must be derived from the output of the risk assessment/ risk treatment plan and, if ISO 27001 compliance is to be achieved, must directly relate the selected controls back to the original risks they are intended to mitigate. • For each risk, the options for treatment are must be evaluated (e.g. applying controls, accepting, avoiding or transferring risks) and actions are performed based on the selected option. Management approval is needed for each situation where risks are accepted. • A Statement of Applicability identifies whether each of the controls defined within Annex A of the ISO 27001 (or other relevant controls) standard will be applied or not based on the Risk Treatment Plan.

Documents reviewed	N/a

Do stage

Risk Treatment Plan	
Short description	Formulate and implement a Risk Treatment Plan that outlines the management action, resources, responsibilities and priorities needed to achieve the plan.
UD Observations	● The organization has not documented the requirements for Risk Treatment Plan creation and has not created Risk Treatment Plan template.
UD Observation Ranking	Major non-conformity
Recommendations	● Develop a comprehensive Risk Treatment Plan that would include: - Appropriate management action. Management should agree with the Risk Treatment Plan and approve any risk acceptances. - Resources. Management should assign resources (e.g. man-hours or budget) which can achieve the treatment of risk. - Responsibilities for treatment. A responsible person/team should be identified who will manage the treatment process. - Priorities for treatment. It should be identified which Risks are treated first; usually this will be the highest risks which take the least amount of effort to mitigate. - Due date: Although this is not a required field, we recommend including it to set expectations regarding when actions will be achieved. ● According to the document Risk Treatment Plan (in fact – Risk Assessment Report) should document identified risks and the decisions about how each of the identified risks should be handled. ● Document detailed requirements for Risk Treatment (Action) Plan creation. ● Annually review and re-approve the Risk Treatment document with management based on the outcomes of the Risk Assessment.
Documents reviewed	N/a

Check stage

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

Act stage

ISMS Improvement including Corrective & Preventive Actions	
Short description	After the Check phase (including several management reviews and the Internal Audit), the ISMS should be improved through corrective & preventive actions.
UD Observations	● The organization has not developed a document which describes the activities that should be taken at each stage of ISMS implementation at [CLIENT], including "Act" stage.
UD Observation Ranking	Major non-conformity
Recommendations	● [CLIENT] has to document Corrective and Preventive Action procedure which is aimed to ensure that problems, non-conformities, and improvements are dealt with in an efficient and effective manner, minimising the chances of any recurrence. ● Corrective and preventative actions should be documented in a consolidated repository or document after they are identified and should include: - A description of the non-conformity (or potential non-conformity) - A root-cause analysis of the non-conformity - The actions needed to prevent recurrence - The status of the action item - The actions identified should be implemented and the plan should be updated with the current status of the action - The target date for implementation ● The corrective and preventative actions and any improvements undertaken should be communicated to interested or impacted parties and management should confirm that these improvements/ actions achieve the intended objectives. ● After the identification of the need for improvements or non-conformities through management reviews, Internal Audits, and other reviews, the corrective and preventive action plan should be updated and regularly reviewed by management.
Documents reviewed	N/A

Recommendations – Annex A controls

The tables on the subsequent pages include recommendations for improvements to the Annex A controls. These recommendations were identified based on a review of the current state ISMS capabilities at [CLIENT]. The recommendations are grouped by processes and as a result, multiple Annex A controls may be addressed within each table.
These tables represent recommendations only and [CLIENT] management will need to ultimately decide what actions to undertake to add or improve the Annex A controls that support their ISMS.

A.5 Information Security Policies

A.5.1 Management direction for information security	
Short description	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
ISO 27001 Control	A.5.1.1. Policies for information security A.5.1.2. Review of the policies for information security
UnderDefense Observations	● [CLIENT] doesn't utilize separate Security Policies. There are Standard Operating Procedures (SOP) covering different industry domains. Most of security procedures are described in Logical and Physical Security SOP. ● All SOPs are reviewed annually. If there is a special request, the policy will be reviewed immediately.
UnderDefense Observation Ranking	Major non-conformity
Recommendations	● Divide information security policy into topic-specific policies, which further mandate the implementation of information security controls and are typically structured to address the needs of certain target groups within an organization or to cover certain topics. (e.g mobile devices and teleworking, cryptographic controls, antivirus controls, management of technical vulnerabilities etc.)
Documents reviewed	[CLIENT]_Quality_Manual [CLIENT]_SOP501_Logical_and_Physical_Security

A.6 Organisation of Information Security

A.6.1 Internal Organisation	
Short description	To establish a management framework to initiate and control the implementation and operation of information security within the organization.
ISO 27001 Control	A.6.1.1 Information security roles and responsibilities A.6.1.2 Segregation of duties A.6.1.3 Contact with authorities A.6.1.4 Contact with special interest groups A.6.1.5 Information security in project management
UnderDefense Observations	• Senior management is responsible for establishing, maintaining and enforcing information security policies within the Company. Security strategies and policies are approved by IT Director, Production Director, PMO Director, Quality Assurance and Compliance Director. They are reviewed annually or if any incidents recorded pose any vulnerability which is not defined or mentioned in security policies. • HR department is responsible for familiarization newcomer employees with all instructions which related to workflow. • QA and Compliance director is responsible for coordination and ideological direction of procedures. IT department is responsible for implementation and adherence to policies. • Based on the results of Assessment, the organization did not identify need of establishing contacts with relevant authorities. Currently information security incidents are investigated internally. • [CLIENT] has requested the UnderDefense, as an independent and trusted Cyber Security partner, conducts an assessment and analysis of the current state of the information security level of the organization. • [CLIENT] has a procedure, which describes that a risk assessment should be performed for each project to identify the potential risks and a risk mitigation plan should be elaborated for each risk identified to prevent risk high effects. But on practice, all security checks are carried out if the client himself wishes this for the prior consent and for the additional payment.
UnderDefense Observation Ranking	Minor non-conformity
Recommendations	• Appoint an owner for each policy who then becomes responsible for its day-to-day implementation.

Documents reviewed	[CLIENT]_SOP901_Corrective_and_Preventive_Actions

A.6.2 Mobile devices and teleworking	
Short description	To ensure the security of teleworking and use of mobile devices. Teleworking refers to all forms of work outside of the office, including non-traditional work environments, such as those referred to as “telecommuting”, “flexible workplace”, “remote work” and “virtual work” environments.
ISO 27001 Control	A.6.2.1 Mobile device policy A.6.2.2 Teleworking
UnderDefense Observations	● QA department uses mobile devices which are utilized for mobile application testing. There is informal rule that says not to bring these devices out of office, but no documented policies or procedures. ● [CLIENT] doesn’t utilize any MDM or MAM solutions. ● [CLIENT] doesn’t have a policy that defines the conditions and restrictions for using teleworking. Most of employees work on corporate laptops, there are also employees who work on their own laptops. Therefore IT department sends email template with requirements for laptop and work process to each newcomer. ● IT department does general check whether antivirus and automatic software update are turned on on each laptop: corporate or private. ● There is no BYOD documented policy. ● Employees are allowed to work remotely connecting to corporate VPN with domain credentials. ● There is no policy or procedure describing usage of public Wi-Fi networks.
UnderDefense Observation Ranking	Major non-conformity
Recommendations	● Implement document named Teleworking policy to ensure that teleworking is undertaken safely from an information security perspective Describe teleworking activities, acceptable use of information processing facilities, guidelines in the use of public Wi-FI networks and prohibited activities.
Documents reviewed	[CLIENT]_SOP501_Logical_and_Physical_Security.pdf

A.7 Human resources security

A.7.1 Prior to employment	
Short description	To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.
ISO 27001 Control	A.7.1.1 Screening A.7.1.2 Terms and conditions of employment
UnderDefense Observations	● [CLIENT] uses policy with background check procedures. ● Basic prescreening is done before employment - check social networks, such as linkedin, facebook etc. if these links are submitted in CV ● Contracts include confidentiality clauses are signed between staff and contractors. Also, NDAs are signed for Employees prior joining the company. ● Terms and conditions of employment are documented in Employee Handbook, Onboarding and Adaptation Procedure.
UnderDefense Observation Ranking	Conforms
Recommendations	N/A
Documents reviewed	Background Check Policy and Procedure Employee_Handbook_2018 NDA - [CLIENT] Onboarding and Adaptation Procedure

A.7.2 During employment	
Short description	To ensure that employees and contractors are aware of and fulfil their information security responsibilities.
ISO 27001 Control	A.7.2.1 Management responsibilities A.7.2.2 Information security awareness, education and training A.7.2.3 Disciplinary process
UnderDefense Observations	● [CLIENT] regularly conducts trainings for its employees, but not Information Security training, Security Awareness etc. ● Manager, Team lead, Project Manager sends email with general advices describing best work practises related to direction (QA, Software Development, DevOPs) including security practices. ● [CLIENT] is carrying out audits to follow the safe working process of employees.

	● Head of recruiting department conducts training for recruiting employees based on instructions which describes in NDA ● [CLIENT] didn't document procedures describing the disciplinary process in case of violation neither conditions of NDA nor IT security practices overall. ● In case of information security incident, the employee receives a letter (informal reprimand) with all details, and also a conversation is conducted with employee with respect to this violation.
UnderDefense Observation Ranking	Major non-conformity
Recommendations	● Implement document named Security Awareness policy that defines scope, procedures, topics, roles and responsibilities in terms of Awareness program. ● Document and implement disciplinary process that are designed to provide a structured corrective action process to improve and prevent a recurrence of undesirable employee behavior and performance issues.
Documents reviewed	N/a

A.8 Asset management

A.8.1 Responsibility for assets	
Short description	To identify organizational assets and define appropriate protection responsibilities.
ISO 27001 Control	A.8.1.1 Inventory of assets A.8.1.2 Ownership of assets A.8.1.3 Acceptable use of assets A.8.1.4 Return of assets
UnderDefense Observations	• [CLIENT] keeps an inventory of devices, books, access cards, which are issued to an employee. • Inventorisation of all assets associated with information and information processing facilities is carried out in form of Excel table with a detailed description of an asset and link to the owner. The table is updated manually by IT department every time new asset is given. • There is no policy on acceptable use of technology resources such as instant messaging, browser extensions etc. • The employee resignation policy lacks procedure that would describe return the organisation's assets on termination of employment, namely corporate laptop and smartphone.
UnderDefense Observation Ranking	Major non-conformity
Recommendations	• Document and implement a formal policy which establishes assets inventory and methods of inventory whether it is conducted manually or with help of automatic tools. For each asset organization must document sufficient information to identify the asset, its physical (or logical) location, information security classification. • Document and implement procedures acceptable use of applications, hardware, information and other information technology resources and systems.
Documents reviewed	[CLIENT]_SOP501_Logical_and_Physical_Security.pdf Employee resignation procedure.docx

Inventory tools to install (as a recommendation)	The are free System and Software inventory tools from ManageEngine to collect information about the software and system information in a given computers of a Windows Domain. The list of installed software on each domain member can be imported in .csv file by one click. You can utilize Nessus Professional (if you use it as a Vulnerability Scanner) as raw host inventory tool. You can launch Host Discovery scan within your

	corporate network to discover all live host and open ports.

A.8.2 Information Classification	
Short description	To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.
ISO 27001 Control	A.8.2.1 Classification of information A.8.2.2 Labelling of information A.8.2.3 Handling of assets
UnderDefense Observations	● The process of information sharing is guided by "Need to know" basis. Document Control procedures, namely Paper Documentation chapter describes what paper documents should be considered as confidential. [CLIENT] doesn't have policy covering classification of digital information. ● Document Control procedures, namely Document Design chapter covers labelling of information. ● [CLIENT] doesn't have any procedures or policies related to handling of assets for each information classification.
UnderDefense Observation Ranking	Major non-conformity
Recommendations	● Add procedures describing classification of digital information which aims to ensure that information is handled according to the risk or impact to ensure the confidentiality, integrity and availability of data.
Documents reviewed	[CLIENT]_SOP601_Document_Control.pdf

A.8.3 Media handling	
Short description	To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.
ISO 27001 Control	A.8.3.1 Management of removable media A.8.3.2 Disposal of media A.8.3.3 Physical media transfer
UnderDefense Observations	● [CLIENT] does not have procedures or policies regulating removable drives like USB or external hard drives. ● [CLIENT] does not have procedures describing how are media disposed-of. If there is a special request from a customer, the media drive will be destroyed permanently.

UnderDefense Observation Ranking	Major non-conformity
Recommendations	• Create Removable Media Policy to minimize the risk of loss or exposure of sensitive information maintained by [CLIENT] and to reduce the risk of acquiring malware infections on computers operated by [CLIENT]. Document and implement procedures that would prohibit or allow acceptable usage of USB flash memory or external hard drives, define roles and responsibilities.
Documents reviewed	[CLIENT]_SOP601_Document_Control.pdf

A.9 Access control

A.9.1 Business requirements for access control	
Short description	To limit access to information and information processing facilities.
ISO 27001 Control	A.9.1.1 Access control policy A.9.1.2 Access to networks and network services
UnderDefense Observations	• Access control procedures described within Logical and Physical Security. • [CLIENT] has document policy which describe access to networks and network services (VPN, Wi-Fi). • Core Value does not have documented policy or procedures which describe access control to Atlassian Jira and Confluence, CoreBase etc.
UnderDefense Observation Ranking	Minor non-conformity
Recommendations	• Bring Access control procedures in a separate policy. • Define who may access the services such as Atlassian Jira and Confluence, CoreBase provided by [CLIENT], and describe the logical access conditions to those services.
Documents reviewed	[CLIENT]_SOP501_Logical_and_Physical_Security

A.9.2 User access management	
Short description	To ensure authorized user access and to prevent unauthorized access to systems and services.
ISO 27001 Control	A.9.2.1 User registration and de-registration A.9.2.2 User access provisioning

	A.9.2.3 Management of privileged access rights A.9.2.4 Management of secret authentication information of users A.9.2.5 Review of user access rights A.9.2.6 Removal or adjustment of access rights
UnderDefense Observations	• User registration and de-registration described in Onboarding and Adaptation, Employee resignation procedures. • Several administrator privileges, such as installing new software, granted to Microsoft Active Directory users or groups to perform certain operations. • [CLIENT] doesn't have procedures regulating employees privileged access rights. • Project Manager, Team Lead, are responsible for giving certain permissions on projects.
UnderDefense Observation Ranking	Minor non-conformity
Recommendations	• Instead of giving Active Directory users local admin rights, limit it to certain number of rights via creating new organizational unit (OU). Organizational Units allow you to delegate admin tasks to users/groups without having to make him/her an administrator. • Please refer to **A.9.3.1** control regarding Management of secret authentication information. • Add procedures which would describe removal or adjustment of access rights during changes of employment.
Documents reviewed	[CLIENT]_SOP501_Logical_and_Physical_Security.pdf Employee resignation procedure.docx Onboarding and Adaptation Procedure.docx

A.9.3 User responsibilities	
Short description	Users should be required to follow the organization's practices in the use of secret authentication information.
ISO 27001 Control	A.9.3.1 Use of secret authentication information
UnderDefense Observations	• There are no documented procedures requiring usage of password managers from all employees. • KeePass password manager is used by IT and DevOps departments.
UnderDefense Observation Ranking	Major non-conformity

Recommendations	• Document and implement policy that outlines the need for well thought out password protection(e.g usage of password managers: KeePass, OnePassword)
Documents reviewed	[CLIENT]_SOP501_Logical_and_Physical_Security

Password managers to install (as a recommendation)	• KeePassX - free, open source, cross platform password manager. Supports multifactor authentication to your passwords database. KeePass being open source means that a number of people have reviewed the code and found it to be secure. • 1Password - commercial password manager. The main advantage is that you can install app on all your devices and sync your password database. 1Password Teams allows you to share password between certain group of people. There are admin controls to view and manage permissions to each shared password.

A.9.4 System and application access control	
Short description	To prevent unauthorized access to systems and applications.
ISO 27001 Control	A.9.4.1 Information access restriction A.9.4.2 Secure log-on procedures A.9.4.3 Password management system A.9.4.4 Use of privileged utility programs A.9.4.5 Access control to program source code
UnderDefense Observations	• Access to information and application systems such as Corebase, Atlassian Jira and Confluence, VPN are protected with authorization. • All [CLIENT] employees have Multifactor authentication configured on corporate G-mail account, it is informal rule, no documented procedures describing usage of MFA. • [CLIENT] does not have procedures restricting the use of system utilities. Active Directory users have privileged rights (see **A.9.2**). • Access control to program source code mostly covered by GitHub, GitLab, BitBucket version control systems. No documented procedures, such as enabling MFA for version control systems.
UnderDefense Observation Ranking	Major non-conformity
Recommendations	• Please refer to **A.9.2.3** control regarding Use of privileged utility programs.

	● Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also. ● Please refer to **A.9.3.1** control regarding Password management systems.
Documents reviewed	N/a

A.10 Cryptography

A.10.1 Cryptographic controls	
Short description	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
ISO 27001 Control	A.10.1.1 Policy on the use of cryptographic controls A.10.1.2 Key management
UnderDefense Observations	● There is no documented policy on the use of cryptographic controls. Consequently neither documented framework nor related controls were established. ● There are no procedures that would define rules of Full Disk Encryption usage. ● SSL/TLS certificates are purchased from Symantec. ● Key management process is not regulated within the organization.
UnderDefense Observation Ranking	Major non-conformity
Recommendations	● Develop and implement cryptographic controls policy to establish requirements and procedures for the use of encryption techniques to protect sensitive data. Assign roles and responsibilities, e.g. who is responsible for: 1) the implementation of the policy; 2) the key management, including key generation. ● Develop and implement policy or procedures needed to create, manage, distribute, use, store, and revoke cryptographic keys and digital certificates(e.g. public key infrastructure (PKI))
Documents reviewed	N/a

A.11 Physical and environmental security

A.11.1 Secure areas	
Short description	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.
ISO 27001 Control	A.11.1.1 Physical security perimeter A.11.1.2 Physical entry controls A.11.1.3 Securing offices, rooms and facilities A.11.1.4 Protecting against external and environmental threats A.11.1.5 Working in secure areas A.11.1.6 Delivery and loading areas
UnderDefense Observations	• There are surveillance CCTV cameras installed on all floors, entrances and exits. • Physical access control is implemented. A physical log book is maintained by receptionist. There is no electronic logging of each employee. • Paper documents are stored in-house in special locked room. There is a defined group of people who have access to this room. • Central alert system is configured. Informal procedures for alert of disaster are present. • Physical security is outsourced on separate specialized company. There is a guard on duty at the main entrance. The guard is responsible for alerting in case of emergency situation or natural disaster. There is a record of alert message which is played.
UnderDefense Observation Ranking	Minor non-conformity
Recommendations	• Install an electronic logging of each employee to ensure that only authorized personnel are allowed access to certain organization premises.
Documents reviewed	[CLIENT]_SOP501_Logical_and_Physical_Security.pdf

A.11.2 Equipment	
Short description	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.
ISO 27001 Control	A.11.2.1 Equipment siting and protection A.11.2.2 Supporting utilities A.11.2.3 Cabling security

	A.11.2.4 Equipment maintenance A.11.2.5 Removal of assets A.11.2.6 Security of equipment and assets off-premises A.11.2.7 Secure disposal or reuse of equipment A.11.2.8 Unattended user equipment A.11.2.9 Clear desk and clear screen policy
UnderDefense Observations	• Equipment is sited in the protected areas which are equipped with: - air conditioning system - security alarm - fire alarm system - video surveillance system - card controlled entry gates - mechanical lock • Equipment is protected from power failures by UPS. • The organization purchases services of local laptop repair company. There are no documented procedures of equipment maintenance outside the organization's premise. Consequently neither documented framework nor related controls were established. • The organization does not perform verification of equipment prior to disposal in order to ensure that any sensitive data and licensed software has been removed or securely overwritten. • Managers practise informal verbal notification about screen locking, no related documented procedures were established.
UnderDefense Observation Ranking	Major non-conformity
Recommendations	• Create and document procedures defining correct equipment maintenance outside the organization's premise. Confidential information should be cleared from the equipment or full disk encryption(FDE) must be enabled . • Establish, document and implement Clean Desk Policy to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. • Document secure disposal procedures to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. Confidential information can be compromised through careless disposal or re-use of equipment.
Documents reviewed	Typical Hardware models.xlsx Workstation.xlsx

A.12 Operations security

A.12.1 Operational procedures and responsibilities	
Short description	To ensure correct and secure operations of information processing facilities.
ISO 27001 Control	A.12.1.1 Documented operating procedures A.12.1.2 Change management A.12.1.3 Capacity management A.12.1.4 Separation of development, testing and operational environments
UnderDefense Observations	● The organization has defined requirements for documenting of operating procedures within organization. Some of operational procedures are documented selectively. ● Change management process within the organization is regulated by Change Management SOP. The following key areas are covered by the policy: - Software Change Control - Document Change Control - Contractual Change Control ● Capacity management is represented for current state, there is an Excel table with all hardware models, also each newcomer get predefined documented pack of hardware. ● There is no policy of capacity projections which describes purchase plan for the next year.(Purchase plan for laptops, mobile devices, printers, other hardware) ● The organization developed and adopted Test Procedures policy. It states that test environment should be set up as a separate automatic test system (ATS) architecture.
UnderDefense Observation Ranking	Minor non-conformity
Recommendations	● Create and document capacity projections which describes purchase plan for the next year. ● Create and document comprehensive description of separation of development, testing and operational environments.
Documents reviewed	[CLIENT]_SOP601_Document_Control [CLIENT]_SOP903_Change Management [CLIENT]_SOP301_Test_Procedures [CLIENT]_SOP402_Unit_Testing Typical Hardware models.xlsx Workstation.xlsx [CLIENT]_network_diagram.pdf

A.12.2 Protection from malware	
Short description	To ensure that information and information processing facilities are protected against malware.
ISO 27001 Control	A.12.2.1 Controls against malware
UnderDefense Observations	• The organization has adopted Anti-virus procedures which regulates protection against malicious code execution. It states that all All [CLIENT] computers should have standard, supported anti-virus software. Workstations which run licensed Microsoft Windows 10 have Windows Defender Antivirus, certain number of workstations run trial ESET NOD32 Antivirus.
UnderDefense Observation Ranking	Major non-conformity
Recommendations	• Establishing a formal policy describing protection against malware. • Install and regular update malware detection and repair software to scan computers and media as a precautionary control, or on a routine basis; the scan carried out should include: 1) scan any files received over networks or via any form of storage medium, for malware before use; 2) scan electronic mail attachments and downloads for malware before use; this scan should be carried out at different places, e.g. at electronic mail servers, desktop computers and when entering the network of the organization; 3) scan web pages for malware;
Documents reviewed	[CLIENT]_SOP501_Logical_and_Physical_Security

Antivirus tools to install (as a recommendation)	ESET Security Management Center - an enterprise antivirus solution, provides on-premise and off-premise endpoints antivirus monitoring and protection whether it is Windows, MacOS, Linux, Android or iOS. The Security Management Center provides an administrator with admin panel (e.g Server Manager in Windows Server) where security events from all endpoints are collected and can be analysed. Admin panel unify all administrator tasks and significantly improves remediation actions within corporate perimeter. One main advantage of ESET Security Management Center is that performance can be improved in combination with such orchestration solutions like Demisto or Firebase. Basically, administrative tasks can be automated with help of so-called Playbooks - predefined scenarios that the system follows. The main goal is to minimize further damage to information assets and timely response to the intrusion.

	For example, a system can be configured in a way when it prevents ransomware from encrypting the files.

A.12.3 Backup	
Short description	To protect against loss of data
ISO 27001 Control	A.12.3.1 Information backup
UnderDefense Observations	● Back-up process is regulated by a formal policy which describes requirements to backup/restore procedures (retention time, backup frequency, backup method) according to classified types of information.. Following information is backed-up according to the policy: - SQL production and development databases - Source code, related object files and configuration files - Software Development Life Cycle documentation - Issue tracking system - Contracts, financial files, other mission-critical business documents - Server disk images ● Every month there are reviews on inactive projects on GitHub, GitLab, BitBucket. Inactive projects are archived and backuped. ● The organization has not defined requirements for regular execution of backup recoverability testing procedures as well as instructions for their execution.
UnderDefense Observation Ranking	Minor non-conformity
Recommendations	● Implement and document procedures describing regular testing of backup media to ensure that they can be relied upon for emergency use when necessary; this should be combined with a test of the restoration procedures and checked against the restoration time required.
Documents reviewed	[CLIENT]_SOP701_Back-up_and_Storage

A.12.4 Logging and monitoring	
Short description	To record events and generate evidence.

ISO 27001 Control	A.12.4.1 Event logging A.12.4.2 Protection of log information A.12.4.3 Administrator and operator logs A.12.4.4 Clock synchronisation
UnderDefense Observations	● Logs of successful and unsuccessful log-on activities, events of modification of network equipment configuration are maintained by embedded functionality of network devices ● Event logging is enabled on MikroTik Routers and Synology NAS. ● There is no formal policy which regulates types of logs which should be maintained and monitored within organization is in place, formal requirement to specific events which should be contained in these logs, logs retention periods, responsibilities of key process participants are not defined.
UnderDefense Observation Ranking	Major non-conformity
Recommendations	● Develop, document, implement, and maintain effective log management policy/procedures throughout the company.
Documents reviewed	N/a

A.12.5 Control of operational software	
Short description	To ensure the integrity of operational systems.
ISO 27001 Control	A.12.5.1 Installation of software on operational systems
UnderDefense Observations	● IT department sends an email with general recommendations not to install software which is not related directly to work procedures. ● There is no documented procedures that would require users of workstations install software only from approved "White software list". ● Installation of software on local operating systems is not properly controlled within organization. IT Department uses unlicensed “Admin inventory” tool to monitor and control Microsoft Active Directory users.
UnderDefense Observation Ranking	Major non-conformity
Recommendations	● Develop and implement procedures/controls for approving/restricting software installation on operating systems for user workstation. To restrict users possibility to install software on operating systems implement preventive technical controls, or detective procedures of checking software which is already installed.

Documents reviewed	N/a

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 [CLIENT] deems as acceptable and unacceptable software that is installed (e.g. whitelists)
Documents reviewed	[CLIENT]_SOP501_Logical_and_Physical_Security

Vulnerability management tools to install (as a recommendation)	Nessus Professional - a vulnerability assessment solution with the lowest false positive rate. Main advantages: • Ability to create and run custom scan. • Nessus is partly proprietary - ability to write and add your own rules. • Ability to import scan report to .csv or .pdf files. • Intuitive and user-friendly interface, so you can install and start to scan your corporate perimeter immediately.

A.12.7 Information systems audit considerations	
Short description	To minimise the impact of audit activities on operational systems.
ISO 27001 Control	A.12.7.1 Information systems audit controls
UnderDefense Observations	• Based on the results of Assessment, the organization did not identify any business needs of Information systems audit. Consequently neither documented framework nor related controls were established.
UnderDefense Observation Ranking	Cannot be assessed
Recommendations	N/a
Documents reviewed	N/a

A.13 Communications security

A.13.1 Network security management	
Short description	To ensure the protection of information in networks and its supporting information processing facilities
ISO 27001 Control	A.13.1.1 Network controls A.13.1.2 Security of network services A.13.1.3 Segregation in networks
UnderDefense Observations	• A network segmentation is implemented. Network is divided into separate network domains: DMZ, Guest network, Internal network. Third party users and contractors work in guest network where access from other networks is restricted. The segregation is done by using different logical networks (e.g.virtual private networking). • [CLIENT] has established MAC filtering for internal wired and wireless connections. The process of aggregating MAC-addresses is in form of Excel file. • Access between network domains is controlled at the perimeter using a gateways (e.g. firewall, filtering router) • Despite the fact that organization has implemented set of network controls, formal documentation of controls configuration requirements is not established.
UnderDefense Observation Ranking	Minor non-conformity

Recommendations	• Create formal documentation of network controls configuration.
Documents reviewed	[CLIENT]_network_diagram.pdf connections-diagram updated.vsdx

A.13.2 Information transfer	
Short description	To maintain the security of information transferred within an organization and with any external entity
ISO 27001 Control	A.13.2.1 Information transfer policies and procedures A.13.2.2 Agreements on information transfer A.13.2.3 Electronic messaging A.13.2.4 Confidentiality or nondisclosure agreements
UnderDefense Observations	• There are no documented procedures that ensure that information is protected against unauthorized access, misuse or corruption during transfer. Neither documented framework nor related to information transfer controls were established. • There are no documented procedures describing transfer of secret authentication information, namely passwords. • [CLIENT] signs nondisclosure agreements with employees, clients and third parties.
UnderDefense Observation Ranking	Major non-conformity
Recommendations	• Establish, document and implement policy that lays out the practical methods that need to be applied in undertaking a transfer of information. • Establish and document guidelines for electronic messaging usage which make users aware of what [CLIENT] deems as acceptable and unacceptable use of its messaging process.
Documents reviewed	NDA - [CLIENT].docx NDA(eng) 2018.docx

A.14 System acquisition, development and maintenance

A.14.1 Security requirements of information systems	
Short description	To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.
ISO 27001 Control	A.14.1.1 Information security requirements analysis and specification A.14.1.2 Securing application services on public networks A.14.1.3 Protecting application services transactions
UnderDefense Observations	● Change management policy which is developed within the organization does not require information security controls specification to be stated in business requirements for new information systems, or enhancements to existing information systems. As a result security requirements are not included in business requirements of information systems occasionally. ●
UnderDefense Observation Ranking	Major non-conformity
Recommendations	● Document and define requirements for new information systems within Project Initiation policy or enhancements to existing information systems within Change Management policy. ● Document usage of secure authentication methods for applications accessible via public networks e.g. using public key cryptography, digital signatures and multifactor authentication to reduce the risks
Documents reviewed	[CLIENT]_SOP102_Project_Initiation.pdf [CLIENT]_SOP903_Change Management.pdf

A.14.2 Security in development and support processes	
Short description	To ensure that information security is designed and implemented within the development lifecycle of information systems.

ISO 27001 Control	A.14.2.1 Secure development policy A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development environment A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System acceptance testing
UnderDefense Observations	● [CLIENT] has Software Development Life Cycle policy which describes following phases: Initiation, Analysis, Design, Development, Testing, Reporting, Maintenance and Archivation. ● Software Development Life Cycle policy states that project objectives, stakeholders, milestones, deliverables, roles and responsibilities, resources, risks, assumption and constraints, high level scope and requirements should be defined as initial steps. ● Thus, there is no documented procedures in Project_Initiation policy describing how risks should be determined. ● The organization has adopted a formal policy which regulates Secure Coding Standard procedures. ● Change management policy which is developed within the organization has Software Change Control that stands for formal change, test and release controls in development lifecycle. ● [CLIENT] implemented three separate network environments, each one for pre-production, development and testing stages. ● Based on the results of assessment, the organization did not identify any risks of service delivery within outsourced software development. Consequently neither documented framework nor related controls were established. ● [CLIENT] has documented Unit Testing policy which is a part of SDLC. ● Test Procedures policy lacks comprehensive description of security testing procedures(OWASP SAMM, etc.)
UnderDefense Observation Ranking	Minor non-conformity
Recommendations	● Integrate Security Testing procedures within your Testing procedures. ● Document and implement detailed procedures defining Static analysis, Dynamic analysis, Fuzz testing. ● Document, apply and implement reviews of software design and software architecture. ● Document, apply and conduct penetration testing procedures on software releases. ● Document and apply Secure Coding Practices Checklist.

Documents reviewed	[CLIENT]_SOP101_Software_Development_Life_Cycle.pdf [CLIENT]_SOP403_Secure_Coding_Standard [CLIENT]_SOP102_Project_Initiation.pdf [CLIENT]_SOP103_Project_Planning.pdf [CLIENT]_SOP401_Code_Review.pdf [CLIENT]_SOP301_Test_Procedures.pdf [CLIENT]_SOP402_Unit_Testing.pdf

A.14.3 Test data	
Short description	To ensure the protection of data used for testing
ISO 27001 Control	A.14.3.1 Protection of test data
UnderDefense Observations	● [CLIENT] doesn't process data containing personally identifiable information or any other confidential information. ● Therefore, based on the results of assessment, the organization did not identify any risks of service delivery within protection of test data. Consequently neither documented framework nor related controls were established.
UnderDefense Observation Ranking	Cannot be assessed
Recommendations	N/a
Documents reviewed	[CLIENT]_SOP301_Test_Procedures.pdf [CLIENT]_SOP402_Unit_Testing.pdf

A.15 Supplier relationships

A.15.1 Information security in supplier relationships	
Short description	To ensure protection of the organization's assets that is accessible by suppliers.
ISO 27001 Control	A.15.1.1 Information security policy for supplier relationships A.15.1.2 Addressing security within supplier agreements A.15.1.3 Information and communication technology supply chain
UnderDefense Observations	● All devices are purchased from authorized distributors. ● [CLIENT] regularly gets certain number of license keys to activate Microsoft Windows operating systems. ● The organization purchases services of local laptop repair company.
UnderDefense Observation Ranking	Minor non-conformity
Recommendations	● Identify and document the types of suppliers, e.g. IT services, logistics utilities, financial services, IT infrastructure components, whom the organization will allow to access its information; ● Identify information security requirements for each type of information and type of access to serve as the basis for individual supplier agreements based on the organization's business needs and requirements. ● Enable full disk encryption (FDE) on laptops which are transferred to laptop repair company.
Documents reviewed	N/a

A.15.2 Supplier service delivery management	
Short description	To maintain an agreed level of information security and service delivery in line with supplier agreements.
ISO 27001 Control	A.15.2.1 Monitoring and review of supplier services A.15.2.2 Managing changes to supplier services
UnderDefense Observations	● Based on the results of assessment, the organization did not identify any business need of monitoring, review, managing changes to supplier services. Consequently neither documented framework nor related controls were established.
UnderDefense Observation Ranking	Cannot be assessed

Recommendations	N/a
Documents reviewed	N/a

A.16 Information security incident management

A.16.1 Management of information security incidents and improvements	
Short description	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.
ISO 27001 Control	A.16.1.1 Responsibilities and procedures A.16.1.2 Reporting information security events A.16.1.3 Reporting information security weaknesses A.16.1.4 Assessment of and decision on information security events A.16.1.5 Response to information security incidents A.16.1.6 Learning from information security incidents A.16.1.7 Collection of evidence
UnderDefense Observations	● The organization has not adopted policy which regulates responsibilities and procedures in terms of information security incidents management process. ● The process of incident response is implemented in issue tracking system Jira. ● The organization has not formal policy which regulates reporting of information security incidents and weaknesses. ● The organization has not documented procedures for learning from information security incidents and collecting evidence.
UnderDefense Observation Ranking	Major non-conformity
Recommendations	● Establish, document, implement and maintain Incident Response Policy. Establish management responsibilities to ensure that the following procedures are developed and communicated adequately within the organization: - procedures for incident response planning and preparation; - procedures for monitoring, detecting, analysing and reporting of information security events and incidents; - procedures for handling of forensic evidence; ● Prepare information security incident submission form to support the reporting action and to help the person reporting to remember all necessary actions in case of an information security event; ● Make aware all employees and contractors of their responsibility to report information security events as quickly as possible. Situations to be considered for information security event reporting include: - ineffective security control; - breach of information integrity, confidentiality or availability expectations; - human errors; - non-compliances with policies or guidelines;

	- breaches of physical security arrangements; - uncontrolled system changes; - malfunctions of software or hardware; - access violations. ● Build an information security incident response team (ISIRT), so that the team assess and make decision on information security events. ● Use anecdotes from actual information security incidents in user awareness training as examples of what could happen, how to respond to such incidents and how to avoid them in the future.
Documents reviewed	N/a

A.17 Information security aspects of business continuity management

A.17.1 Information security continuity	
Short description	Information security continuity should be embedded in the organization's business continuity management systems.
ISO 27001 Control	A.17.1.1 Planning information security continuity A.17.1.2 Implementing information security continuity A.17.1.3 Verify, review and evaluate information security continuity
UnderDefense Observations	• [CLIENT] has Business continuity and Disaster Recovery policy. The policy contains Emergency Management Team, Data and Systems Recovery Timing, Disaster Recovery Activities. The organization defined and adopted two Scenarios for mitigation of emergency situation. • There is an additional reserve switch installed in a server rack for protection against a network failure. • Virtual machines in VMware ESXi hypervisor configured to autostart after a power outage. • All virtual machines are audited by IT department once per quartal.
UnderDefense Observation Ranking	Minor non-conformity
Recommendations	• Regularly exercise and test business continuity plans to ensure that they are remain up to date and effective. • Integrate verification of information security continuity controls with the organization's business continuity or disaster recovery tests.
Documents reviewed	[CLIENT]_SOP902_Business_Continuity_and_Disaster_Recovery

A.17.2 Redundancies	
Short description	To ensure availability of information processing facilities.
ISO 27001 Control	A.17.2.1 Availability of information processing facilities
UnderDefense Observations	• Availability of information processing facilities is protected from power failures and other disruptions by UPS, redundant heating/ventilation and air-conditioning systems.
UnderDefense Observation Ranking	Conforms

Recommendations	• Test redundant information systems to ensure the failover from one component to another component works as intended.
Documents reviewed	N/a

A.18 Compliance

A.18.1 Compliance with legal and contractual requirements	
Short description	To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.
ISO 27001 Control	A.18.1.1 Identification of applicable legislation and contractual requirements A.18.1.2 Intellectual property rights A.18.1.3 Protection of records A.18.1.4 Privacy and protection of personally identifiable information A.18.1.5 Regulation of cryptographic controls
UnderDefense Observations	● The organization makes employees sign personal data processing agreement with clients. ● IT Department uses unlicensed "Admin inventory" tool to monitor and control Microsoft Active Directory users. There is a number of workstations which run unlicensed or outdated versions of Microsoft Windows OS. ● Protection of records is carried out by Data Protection Responsible Person who's in charge of managing internal data protection activities. ● The organization's data protection policy contains Classification Matrix of Personal Data. The Matrix defines Personal Identifiable Information that should be protected. ● Based on the results of assessment, the organization did not identify any risks of regulation of cryptographic controls. Consequently neither documented framework nor related controls were established.
UnderDefense Observation Ranking	Minor non-conformity
Recommendations	● Identify all legislation applicable to the organization in order to meet the requirements for business. If the organization conducts business in other countries, managers should consider compliance in all relevant countries. ● Consider following guidelines to protect any material that may be considered intellectual property: - publish an intellectual property rights compliance policy which defines the legal use of software and information products; - acquire software only through known and reputable sources, to ensure that copyright is not violated; - carry out reviews that only authorized software and licensed products are installed; ● Take the following steps meet record safeguarding objectives: - document guidelines on the retention, storage, handling and disposal of records and information; - draw up a retention schedule identifying records and the period of time for which they should be retained;

	- maintain an inventory of sources of key information ● Data protection policy should be communicated to all persons involved in the processing of personally identifiable information.
Documents reviewed	[CLIENT]_SOP404_Data_Protection.pdf [CLIENT]_SOP601_Document_Control.pdf

A.18.2 Information security reviews	
Short description	To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.
ISO 27001 Control	A.18.2.1 Independent review of information security A.18.2.2 Compliance with security policies and standards A.18.2.3 Technical compliance review
UnderDefense Observations	● The organization SOPs are reviewed annually (see **A.5.1**) ● [CLIENT] does not have the process of periodic independent review of opportunities for improvement and the need for changes to the approach to security. ● Relying on the organization's data protection policy the compliance of information protecting is performed in accordance with NIST 800-122, HIPAA, GDPR standards and regulations. ● The organization didn't document procedures describing a regular review of technical compliance with the organization's information security policies and standards
UnderDefense Observation Ranking	Major non-conformity
Recommendations	● Initiate the independent review of control objectives, controls, policies, processes and procedures for information security at planned intervals or when significant changes occur. ● Review the compliance of information processing and procedures within each managers area of responsibility with the appropriate security policies, standards and any other security requirements. If any non-compliance is found as a result of the review, managers should: - identify the causes of the non-compliance; - evaluate the need for actions to achieve compliance; - implement appropriate corrective action; - review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses. ● Review technical compliance to ensure that hardware and software controls have been correctly implemented. It covers penetration testing and vulnerability assessments, which might be carried out by

	independent experts specifically contracted for this purpose. Such tests should be planned, documented and repeatable.
Documents reviewed	[CLIENT]_SOP404_Data_Protection.pdf

SUMMARY

Within the scope of security assessment for [CLIENT] we conducted several interviews with key stakeholders to value current security level within organization and review existing documentation/policies. After mapping outcomes of interview and documentation analysis on ISO/IEC 27001:2013 controls we evaluated current state of implemented Information Security Management Framework.

We recommend [CLIENT] to start implementing security controls one-by-one to raise them up to recommended level of maturity and in such way cover technical aspects of ISO/IEC 27001 compliance.