UnderDefense

Security Program: Current vs. Future Gap Analysis REPORT for OrganizationXXX

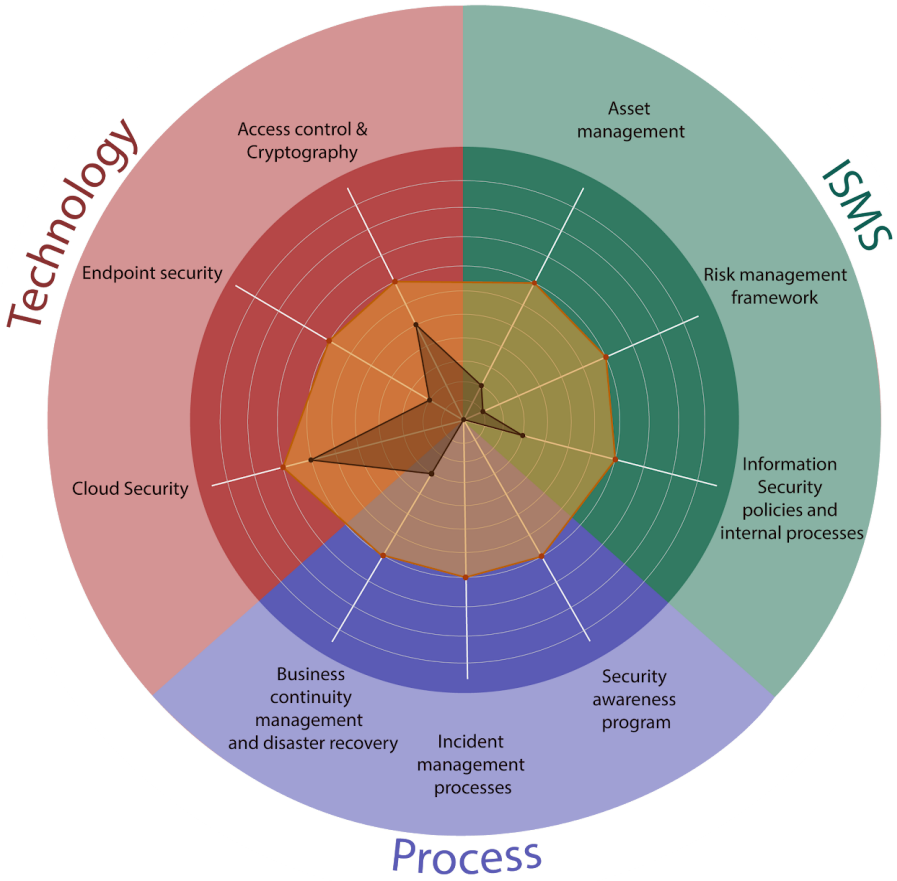
2020

Executive Summary

OrganizationXXX has requested that UnderDefense, as an independent and trusted Cyber Security partner, conduct an assessment and analysis of the current state of the information security level of the OrganizationXXX and its compliance with best practices and CIS20, NIST and GDPR regulations. The main purpose of this Audit was to evaluate business risks associated with cyber security, current processes, available tools, and human resources to meet new EU regulations, readiness to protect employees, and customers from modern attacks, identify gaps, prioritize them by risk level and provide recommendations to close those gaps and mitigate possible future risks. The given recommendations and methodologies are structured due in reference to the identified gaps with an aim of its further mitigation.

Security Program Assessment

The Radar chart below provides a graphical summary of the assessment outcome. This chart describes the current and future levels of managing information security for OrganizationXXX which are related to the Technology-Information, Security-Staff-Process, and main security controls.



This chart consists of 3 major blocks as presented on the image above and represents required steps for a successful transition and achieved compliance with industry certifications such as ISO27001 & GDPR.

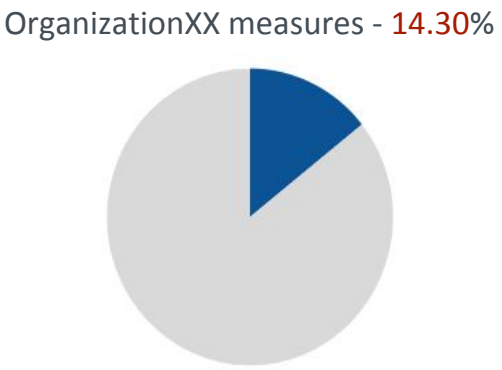
Analysis, description, rating and recommendation for each parameter of this graphical representation detaily reviewed in section "Current security controls analysis".

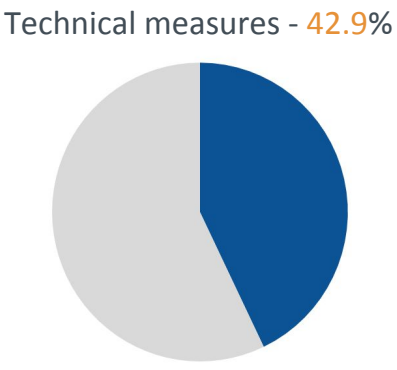
GDPR Readiness results

OrganizationXXX provides outsourcing services engaged with clients that collect, store and process personal data of EU citizens. OrganizationXXX also provides hosting service for testing and production environments with test and real personal data stored in the public cloud and laptops owned by OrganizationXXX employees (personal unencrypted, poorly controlled laptops with poor security governance on them).

This creates situations when failure in security of the weakest employee, may risk entire projects with clients as well as create significant reputational risk for the OrganizationXXX. We also should consider +200 new employees are planned in 2020, this then increasing the risk landscape.

The graphics below reflect the percentage of OrganizationXXX current GDPR Readiness status. There are activities described with details and recommendations provided to reach a certain level of General Data Protection Regulation readiness in the Appendix C table. In order to reach compliance, recommendations should be followed and the processes implemented in a time conscious manner.





Financial risks and budget estimation

We created this section to estimate business and financial risks of failure in the case of a lack of proper security controls in the OrganizationXXX and project base.
Please consider a situation when failure in security of the weakest employee (like peace of code published on stackoverflow or pastebin), may put on risk entire project with clients (e.g. DevOps accidently leaked keys to cloud infrastructure that create a situation when client can be blackmailed, customer data leaked, client fined or whole infrastructure destroyed). Estimated financial risk include only Revenue that might be lost (no fines or liability estimation included)
Financial risk estimation:

Project	xxx	xxx	Revenue monthly	Business Value 1 year	Priority	Investment needed	Investment %	1 year Value
xxx	xxx	xxx	407400	4,888,800.00	High	153,000.00	3.13%	96.87%
xxx	xxx	xxx	138600	1,663,200.00	High	153,000.00	9.20%	90.80%
xxx	xxx	xxx	79800	957,600.00	High	153,000.00	15.98%	84.02%
xxx	xxx	xxx	58800	705,600.00	Medium	153,000.00	21.68%	78.32%
xxx	xxx	xxx	46200	554,400.00	Medium	153,000.00	27.60%	72.40%
xxx	xxx	xxx	42000	504,000.00	Medium	153,000.00	30.36%	69.64%
xxx	xxx	xxx	37800	453,600.00	Low	153,000.00	33.73%	66.27%
xxx	xxx	xxx	33600	403,200.00	Low	153,000.00	37.95%	62.05%
xxx	xxx	xxx	33600	403,200.00	Low	153,000.00	37.95%	62.05%

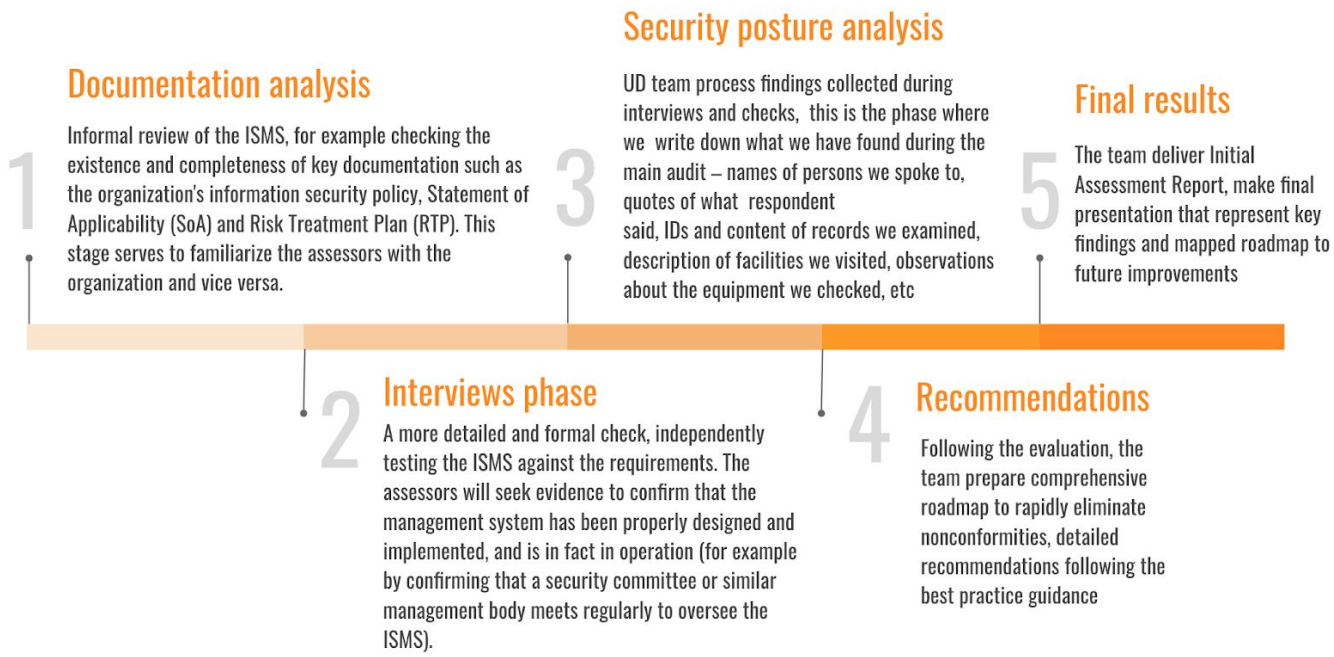
As you can see from the table above, a recommended investment of 153K for 2020 will have significant ROI for most projects/clients served by OrganizationXXX.
Reputation risk estimation:
As reputation is a relational concept this failure can manifest itself in a number of different ways from mild disappointment to extreme outrage. The risk is value based (just as relationships are) not cost based and it cannot be expressed in this way. In the case of a serious security incident and if said incident became public, reputation costs can be also calculated as following:
Let's take as instance 2 prospects for 5 developers might bring OrganizationXXX~ 2,5M in annual revenue, but if reputation will be impacted at least for 3 month (no new deals because of bad reputation) this may converted into 1,2M of indirect loss:

Prospects	Months	Revenue monthly	Impact
2	3	210000	1,260,000.00

As visible from our simple ROI calculation, investment of $153 000 will have a significant value and can increase chances to avoid data breaches, meanwhile minimize risks and allow you to pursue confidently new business opportunities through increased trust and compliance.
OrganizationXXX has functioned for seven years without proper security processes and controls in place. This creates a situation when the current size and structure of the OrganizationXXX cause risks to become extremely high, therefore significant improvement is required.

Our estimated investment budget required in 2020 for tools, processes, and new hires is $153 770.

Steps conducted during Gap Analysis



Information Security Maturity Model

A maturity model is needed to measure the information security processes capabilities. The main objective of such a maturity model is to identify a baseline to start improving the security posture of an organization when conducting GAP analysis.

	LEVEL 1 - PERFORMED	LEVEL 2 - MANAGED	LEVEL 3 - ESTABLISHED	LEVEL 4 - PREDICTABLE	LEVEL 5 - OPTIMIZED
PEOPLE	General personnel capabilities may be performed by an individual, but are not well defined	Personnel capabilities achieved consistently within subsets of the organization, but inconsistent across the entire organization	Roles and responsibilities are identified, assigned, and trained across the organization	Achievement and performance of personnel practices are predicted, measured, and evaluated	Proactive performance improvement and resourcing based on organizational changes and lessons learned (internal & external)
PROCESS	General process capabilities may be performed by an individual, but are not well defined	Adequate procedures documented within a subset of the organization	Organizational policies and procedures are defined and standardized. Policies and procedures support the organizational strategy	Policy compliance is measured and enforced Procedures are monitored for effectiveness	Policies and procedures are updated based on organizational changes and lessons learned (internal & external) are captured.
TECHNOLOGY	General technical mechanisms are in place and may be used by an individual	Technical mechanisms are formally identified and defined by a subset of the organization; technical requirements in place	Purpose and intent is defined (right technology, adequately deployed); Proper technology is implemented in each subset of the organization	Effectiveness of technical mechanisms are predicted, measured, and evaluated	Technical mechanisms are proactively improved based on organizational changes and lessons learned (internal & external)

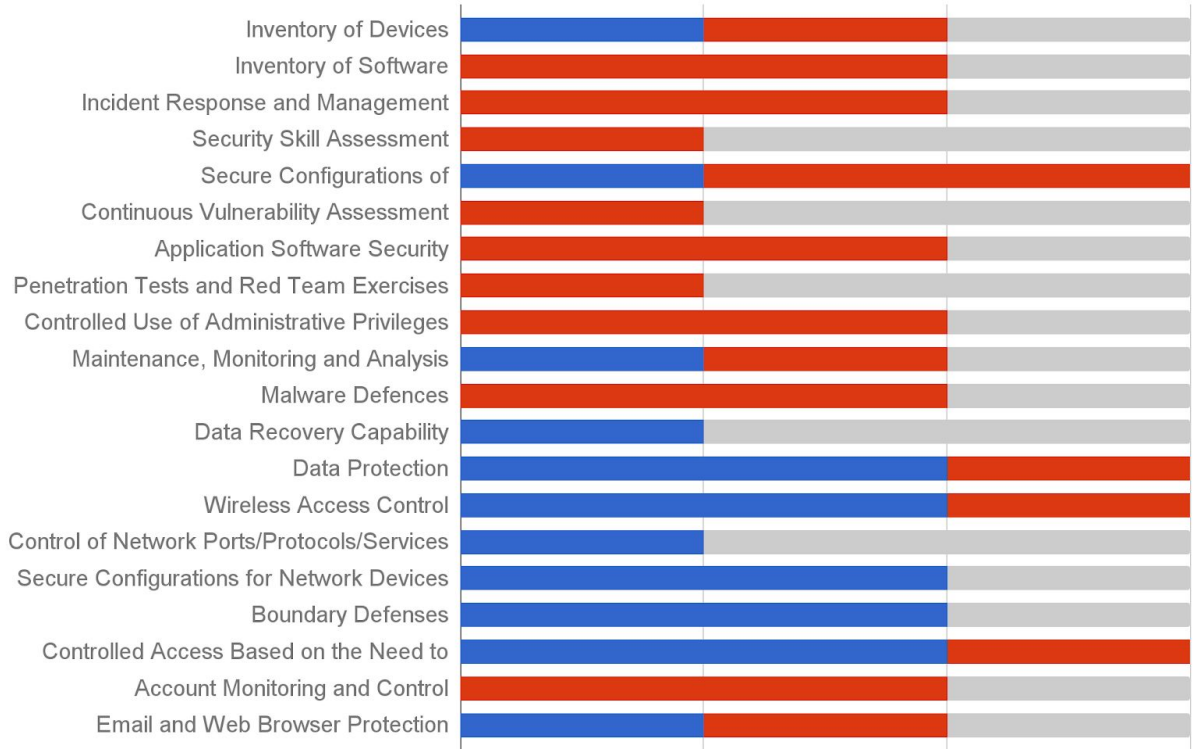
CIS 20 CSC Benchmark

Legend:

Blue line shows - the current state, whereas the red line shows desired state.

For some controls (like Account Monitoring & Control) it's enough to get maturity level 2 (ML2), but as for today OrganizationXXX don't have some of these controls at all (ML0).

A more detailed benchmarking process and recommendations to improve appropriate security controls to minimum required level provided and explained in the Appendix A: Current state of Security Controls according CIS20



Key Cybersecurity Risks identified

More detailed each risk and threat scenario is calculated and represented in Appendix B. OrganizationXXX Cybersecurity Risk Assessment . Please follow the link provided.

Amazon AWS security controls evaluation

Currently 95% of IT Infrastructure is cloud based, so to evaluate security components & controls for Amazon AWS hosted systems and services we utilized automated tools Scout2 & Prowler. Each report and configuration was manually reviewed for each availability zone.

AWS report	
Service	Status
EC2	Medium
S3	Low
Cloud Trail	High
IAM	High
VPC	Medium
SNS	Low

Findings details:

Security documentation analysis

Following policies were assessed during this project:

Document	Status	Details
Dismissal process	Good	This Process is in place, fully simplified, clearly described and available.
Onboarding process	Needs some improvements	Missing a paragraph about employee rotation between the projects. IT department should know where people are placed on project basis to control access rights, technical equipment and readiness of future working places. Other than that this Process is in place, fully simplified, clearly described and available.
Password policy	Good	Security Awareness trainings are needed to inform about terms, obligations and rules of the password policy
User policy	Good	7th paragraph - isn't implemented. 9th paragraph - no backups.
New policies		
Clean desk policy	Is going to be in place	This policy will help your OrganizationXXX reduce the risk of information theft, fraud, or a security breach caused by sensitive information being left unattended and visible in plain view.
Email policy	Is going to be in place	Helps employees use their company email addresses appropriately, understand the limitations of using their corporate email accounts, protect company's confidential data from breaches.
Internet Usage policy	Is going to be in place	This policy provides employees with rules and guidelines about the appropriate use of network and Internet access. Company employees are expected to use the Internet responsibly and productively. Internet access is limited to job-related activities only and personal use is not permitted.

Mobile Device Encryption policy	Is going to be in place	This policy foresees all the mobile devices to be encrypted. It is one of the best ways to secure the most sensitive OrganizationXXXs' data on any type of mobile device. Mobile device encryption offers an easy fix for the problem of data breaches, which are the top threat posed by lost or stolen mobile device.
Virtual Private Network Policy	Is going to be in place	This policy defines standards for connecting to OrganizationXXX's network from hosts on the Internet by using a VPN to the internal network. It's designed to minimize potential exposure from damages which may result from unauthorized use of its resources. Not having this policy in place may lead to damages including the loss of sensitive or confidential data, intellectual property, damage to critical Information & technology systems.
Have to be developed		
Incident Response Plan	Needs to be developed	Incident response plan provides instructions for effective responding to information security incidents. Without an incident response plan in place, the OrganizationXXX may either not detect the attack in the first place, or not follow proper protocol to contain the threat and recover from it when a breach is detected.
Business Continuity Plan	Needs to be developed	It is vital for an OrganizationXXX to have a Business Continuity Plan to preserve its health and reputation. A proper Business Continuity Plan decreases the chance of a costly outage. This plan states the essential functions of the business, identifies which systems and processes must be sustained and how to maintain them.
Project requirements Policy	Needs to be developed	This Policy includes a list of project`s technical requirements and access rights to OrganizationXXX's IT department from Product Manager. This policy ensures that all significant engineering efforts employ approved engineering processes in order to deliver on-time, within-budget, high-quality services to the customers.
Personal data processing policy	Needs to be developed	This policy should be developed utilizing GDPR guidelines and has to include the list of defined procedures about personal data processing (for example what personal data you collect, from which sources you collect it, and with whom it is shared).

GDPR Readiness Status

The General Data Protection Regulation (GDPR) is a Regulation by which the European Commission intends to strengthen and unify data protection for individuals within the European Union. It also addresses export of personal data outside the EU. By “personal data” is meant personally identifiable information (PII) - names, addresses, phone numbers, account numbers, and more recently email and IP addresses.

It addresses the following:

- adding requirements for documenting IT procedures,
- performing risk assessments under certain conditions,
- notifying the consumer and authorities when there is a breach,

- strengthening rules for data minimization.

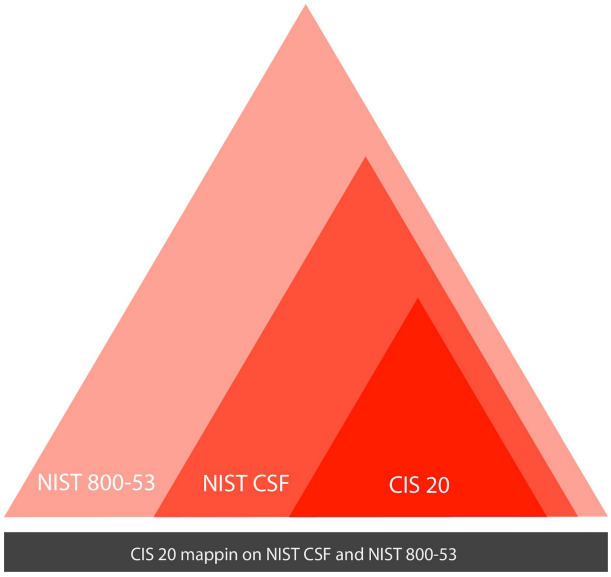
GDPR imposes direct compliance obligations on both controllers and processors, and both controllers and processors will face direct enforcement and serious penalties if they do not comply with the new EU data protection law. Therefore, it is important that processors understand their obligations under EU data protection law.

Based on interviews with key executives in OrganizationXXX, OrganizationXXX NL (as a legal processor on behalf with controller (client)), and all its affiliates, have also full contract responsibility for personal data processing of EU citizens and share responsibility with Controller (client).
Following data was identified in scope of processing by OrganizationXXX and its affiliates: employees' personal data, data of clients' customers used for test and development purposes.

The following procedures currently are not in place but need to be implemented	
Sensitive/Personal Data File Encryption	Not ready
PC/Laptop Full Disk Encryption	Not ready
Email Communication Encryption	OK
Removable Disk Encryption	Not ready
Network/Cloud Folder Encryption	OK

CIS20 current controls summary

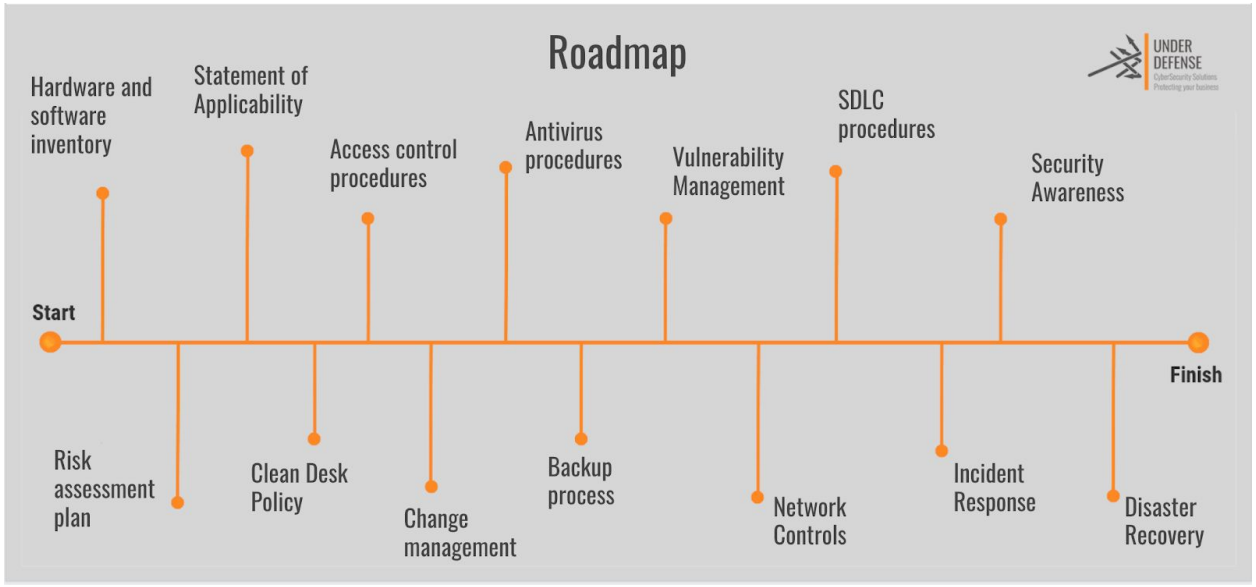
Detailed each control is reviewed in Appendix A.
As for OrganizationXXX, which only begins implementing and designing cybersecurity, we offer to start with CIS 20 Controls, CIS CSC contains important components that make-up an effective cyber defense system, allowing companies to prioritize controls that protect against the greatest threats, provide metrics for IT personnel to understand, continuously diagnose and mitigate risks, and automate defenses to ensure compliance with the controls.
The image below represents how CIS20 covers NIST CSF and NIST 800-53 ISO 27001. While covering CIS 20 controls, you will also cover 70% of NIST CSF controls and almost 50% of NIST 800-53.



Target state as well as GDPR compliance is achievable and detaily described in the Improvement Roadmap section below.

Improvements Roadmap

We recommend dedicating a budget for Security improvements in the amount of minimum $153 000. This amount includes required licenses, tools, processes, tests etc.



Next activities need to be completed to cover most critical vulnerabilities founded during analysis and risk assessment

Status	Phase	Task	Description	Team Members	Due Date
done	Phase 1	Migrate all systems to the AWS		*Alex and X*	8/28/2019
done	Phase 1	Mobile Pentest	Alex will conduct scanning for mobille application code using SonarQube	*X and Alex*	8/28/2019
done	Phase 1	Setup an encrypted VPN connection to the application environment	Configure SSL VPN on FortiGate	*Alex*	8/7/2019
to do	Phase 1	Set up full disk encryption	Full disk encryption software is deployed on all workstations. - Alex will prepare solutions (recommendations) for FDE. - Y and Andrew will set up FDE on each workstation for their teams	*X and Y*	December 2
to do	Phase 1	Set up Anti Virus protection	Anti virus protection software is deployed on all workstations Antivirus is configured for real-time protection and updates to virus signature definitions. - Alex will prepare a solution - recommendations that AV is better to use. - X and Y will set up AV solution on each workstation for their teams	*X and Y*	December 2
to do	Phase 1	Establish regular and qualified vulnerability scanning process	Monthly vulnerability scans are conducted against system resources to identify potential threats. - Alex will prepare a solution for Vulnerability Management (e.g. Tenable.io). - X and Y will deploy VM solution on each workstation and on all other locations where is possible.	*Alex, X and Y*	December 2
to do	Phase 1	Establish regular and qualified patch management process	Patch management is utilized to monitor current patch levels of servers. Critical patches are applied to production servers as needed. - Alex, X, and Y will prepare list of all critical software and hardware related to work with the CRM. - Alex will provide a solution for Patch Management. - X and Y will deploy the PM solution on each workstation and other CRM components where is possible.	*Alex, X, and Y*	December 2
in progress	Phase 1	Conduct Risks Assessment based on ISO 27005 standard	- Alex wil prepare Draft Risk Assessment. - X, Y, and Z will review RA and provide their modifications to it.	*Alex, X, and Z*	November 15
			- X will prepare a secure storage for the sensitive data.		

Prioritized Roadmap

	C	D	E	F	G	H	I	J	K	L
1	Subcategory	Task	Impact on "Unable to release product version"	Impact on "Unable to deliver product version to users/customers"	Impact on "Inability to sell the product"	Impact on "Unable to deliver technical support to our customers"	Impact on "Inability to sell the service"	Impact on "Office unavailability"	Impact on Data Breach	Priority
15	PR.DS-7: The development and testing environment(s) are separate from the production environment	Implement fully functional testing environments, so that test cases can be performed without afraid to cause damage to production environment.	0	3	2	2	2	0	0	199
16	PR.AC-3: Remote access is managed	Set up monitoring remote access to the production system. Allow only authorized use of privileged functions from remote access. Establish agreements and verify security for connections with external systems.	2	2	1	1	1	0	2	194
17	PR.AT-2: Privileged users understand their roles and responsibilities	Establish specific cybersecurity awareness and training procedures for privileged users (e.g. developers) describing acceptable and unacceptable activities at workplace.	2	2	1	1	1	0	2	194
18	PR.DS-1: Data-at-rest is protected	Create and implement procedures which describe how to encrypt all data related to PII within all AWS infrastructure.	0	0	2	1	2	0	3	190
19	PR.AC-2: Physical access to assets is managed and protected	Define, document and implement procedures in Access Control Policy that would describe roles and responsibilities related to physical access. For example: who has to escort fire inspector or air conditioning service during their operations, to what extent, etc;	1	1	1	1	1	3	2	188
20	ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	Define and establish formal procedures describing response, recovery planning and testing with suppliers and third-party providers. Include procedures in contracts: Include in contracts a provision that requires your third-party suppliers/partners to notify you immediately if there is a potential or actual security incident, data security breach.	1	1	2	1	1	0	2	183
21	PR.DS-2: Data-in-transit is protected	Create and implement procedures which will describe how data should be transferred. For example which corporate messenger employees should use for communication or how to correctly obfuscate data before transfer or how to choose a protected way for	1	1	1	1	1	0	3	182

Risk Description	Likeli-hood	C.I.A. Impact	Risk level	Security Control
Unauthorized access to business communication data using social engineering attack	4	4	Critical	Security Awareness training
Unauthorized access to employee desktop using malware attack	4	4	Critical	Advanced Malware Protection
Incident Response rendered ineffective in a timely manner	4	4	Critical	Incident Response process and testing
Unauthorized access to clients' personal and financial information using social engineering attack	4	3	High	SA trainings
Unauthorized access to business communication data using social engineering attack	4	3	High	Security Awareness training
Access to project information after migration to another project	3	4	High	Project migration Policy
Modification of employees' and clients' data because of vulnerabilities in ERP system	3	3	Medium	ERP pentest
Unauthorized access to employee desktop using malware attack	4	2	Medium	Advanced Malware Protection
Unauthorized access to data on the laptop	2	4	Medium	Full disk Encryption
Disclosure of employees' personal data	2	4	Medium	Monitoring of access to any personal data held by organization
Social engineering attack used to get the credentials to access AWS infrastructure, ERP System	4	2	Medium	SA trainings
Site deface	4	2	Medium	Site static pages WAF
Use of existing vulnerability in ERP to access employees' private data	3	2	Medium	ERP pentest

Appendix D: Increase Security of Office 365 for employees

1. Enable MFA for all global admins
2. Enable MFA for all users
3. Enable Client Rules Forwarding Block
4. Advanced Action
5. [Not Scored] Enable audit data recording
6. Review signs-ins after multiple failures report weekly
7. Enable mailbox auditing for all users
8. Review sign-ins from unknown sources report weekly
9. Review signs-ins from multiple geographies report weekly
10. Review role changes weekly
11. Store user documents in OneDrive for Business
12. [Not Scored] Enable Information Rights Management (IRM) services
13. Use audit data
14. Review mailbox forwarding rules weekly
15. Review mailbox access by non-owners report bi-weekly
16. Review malware detections report weekly

APPENDIX E: Key stakeholders interviewed

Prior to initiating our assessment we conducted interviews with the key stakeholder and employees of the OrganizationXXX in order to obtain feedback and to learn about current information security practices, control sets, and risks observed within the OrganizationXXX. The following table shows the list of individuals who took part in the interview, the respondents shared their knowledge of information regarding the state of information security in their OrganizationXXX, presented current controls of information security in their department and answered various questions about security procedures, systems, infrastructure, business processes, policies, growth plans, endpoint security, operating systems, access controls, valuable assets, risks, and other relevant information to the information security state of the OrganizationXXX.

Position in the company	Respondent
CEO	
CFO	
Finance	
Digital Marketing	
ERM	
Operational	
BUM	
BUM	
BUM	
BUM	
HR	
CIO	

When conducting Gap Analysis we identified departments. We divided staff into groups. There are different groups: one has to go through Security Awareness, another - Security Training.

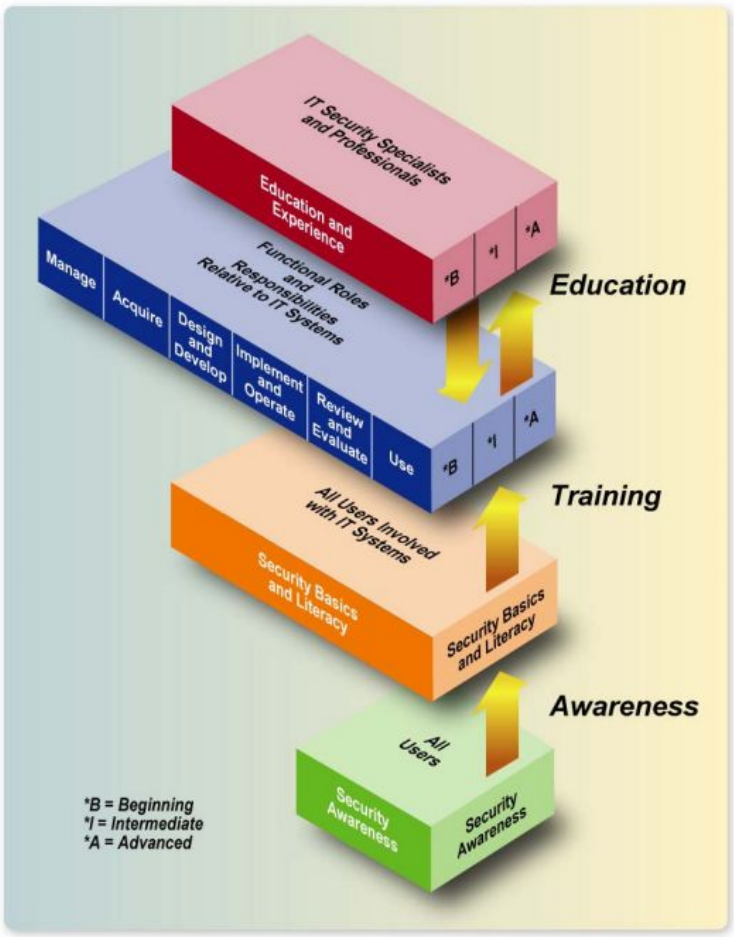


Figure 2-1: The IT Security Learning Continuum

Summary

Within the scope of Gap Analysis for OrganizationXXX we conducted 17 interviews with key stakeholders to value current security levels within the organization and review existing procedures, controls, documentation and policies. After mapping outcomes of interview and documentation analysis on security best practises we evaluated current state company cybersecurity posture. Radar chart was prepared to provide a graphical summary of the assessment. Roadmap was prepared as a step-by-step plan to start executing improvements on the security posture of the organization.
We recommend OrganizationXXX conducting a Risk Assessment, creating Gap elimination plan and to start implementing security controls one-by-one to raise them up to target level of maturity and in such way enable the organization to perform cost-effective, targeted improvements.