



CYBER SCORE

CYBER SCORECARD - DEMO REPORT

Assessment-2



CYBER SCORE



CIS. Center for Internet Security®

Created Date
2021-05-20 23:26:24

1. INTRODUCTION

Information security is of great importance in ensuring the continuity of every organization, and it ensures the protection of critical information and other information assets of the organization in various environments, especially electronic. It should not be forgotten that security will be ensured by investing in people before technology, by raising awareness, by informing, supporting and caring about such matters starting from the top, and security is a process that will be managed continuously. Information security management is a life cycle that should be managed and audited continuously as long as institutions and information exist.

In today's world, in parallel with technological advances, security risks related to information and information technologies are increasing day by day. At the point of ensuring information security, first of all, it should be aimed to determine the information security risks of the institutions and to reduce the existing risks to an acceptable level. On the other hand, internationally accepted standards-rules such as ISO 27001, COBIT, PCI, SOX and BASEL II require risk management in organizations.

Without risk analysis, it causes the countermeasures to be implemented to fail to meet the needs or to cause financial losses by making investments at wrong points.

This report contains the Results of the Cyber Security Maturity Assessment Study conducted for *ABC Bank LLC*. With this study, the adequacy of information security controls applied in the protection of *ABC Bank LLC* information assets, management of information systems infrastructures and business processes were evaluated and weaknesses were identified. Suggestions have also been made to eliminate risks and reduce their effects.

2. ABOUT THE REPORT

2.1. Briefly Frames (CIS 20 Controls v7 and NIST CSF v1.1)

CIS is a non-profit organization that aims to improve cyber security preparedness and responsiveness between public and private sector organizations. CIS contains CIS Critical Security Controls, which shed light on the maturity assessment study we conducted for *ABC Bank LLC* . (<https://www.cisecurity.org/>)

The National Institute of Standards and Technology (NIST) is currently part of the US Department of Commerce. NIST is one of the oldest physical science laboratories in the country.

It offers technology, measurement and standards for countless products and services, from the smart power grid and electronic health records to atomic clocks, advanced nanomaterials and computer chips.

The NIST Cyber Security Framework study is a voluntary guide based on existing standards, guidelines and practices for organizations to better manage and mitigate cyber security risk. It is designed to help organizations manage and mitigate risks, as well as encourage risk and cyber security management communication between internal and external corporate stakeholders. (<https://www.nist.gov/cyberframework/framework>)

2.2. Highlights

ABC Bank LLC IT security infrastructure reflects the basic characteristics of corporate structures. Investments have been made in many different product families. The reasons for the low level of maturity in inventory management, vulnerability / vulnerability management, control of authorized accounts, configuration change management and audit log keeping, which are the top 6 topics recommended by CIS (Center of Internet Security)

- Performing manual work (inventory, vulnerability scans, etc.)
- No PAM solution
- Failure to follow configurations in accordance with a standard

can be counted like. When the recommendations proposed in the conclusion part are implemented, it is thought that high levels of visibility and awareness, which we believe are vital for organizations, will be achieved.

2.3. Key Findings

An Information Security Management program within *ABC Bank LLC* has not yet been completed in terms of policy / procedure.

It was observed that the inventory and patch management was monitored manually on the servers within the *ABC Bank LLC* infrastructure.

Within the infrastructure of *ABC Bank LLC* , it was seen that there were tools that were purchased but not implemented, such as Application Whitelisting and File Integrity Monitoring.

Jobs that can be performed automatically within *ABC Bank LLC* (inventory, vulnerability scans, auditing, etc.) are followed manually. The active use of the SIEM system, especially in terms of visibility, and automating the work will help to take quick action in case of an incident.

2.4. Overview

Frameworks use 1-5 scoring to measure the maturity level of the institution:

- Level 1: High risk level, Unpredictable, Unstable
- Level 2: Responsive, Temporary, Manual tracking
- Level 3: Documented, Repeatable, Standardized
- Level 4: Following metrics, Proactive, Some automation works
- Level 5: Predictable, Automated, Everything integrated

Maturity Level

<div></div>	Level One - Initial	Policies Complete	77.78%
<div></div>	Level Two - Repeatable	Controls 1-5 Implemented	69.87%
<div></div>	Level Three - Defined	All Controls Implemented	76.89%
<div></div>	Level Four - Quantitatively Managed	All Controls Automated	71.93%
<div></div>	Level Five - Optimized	All Controls Reported	71.49%

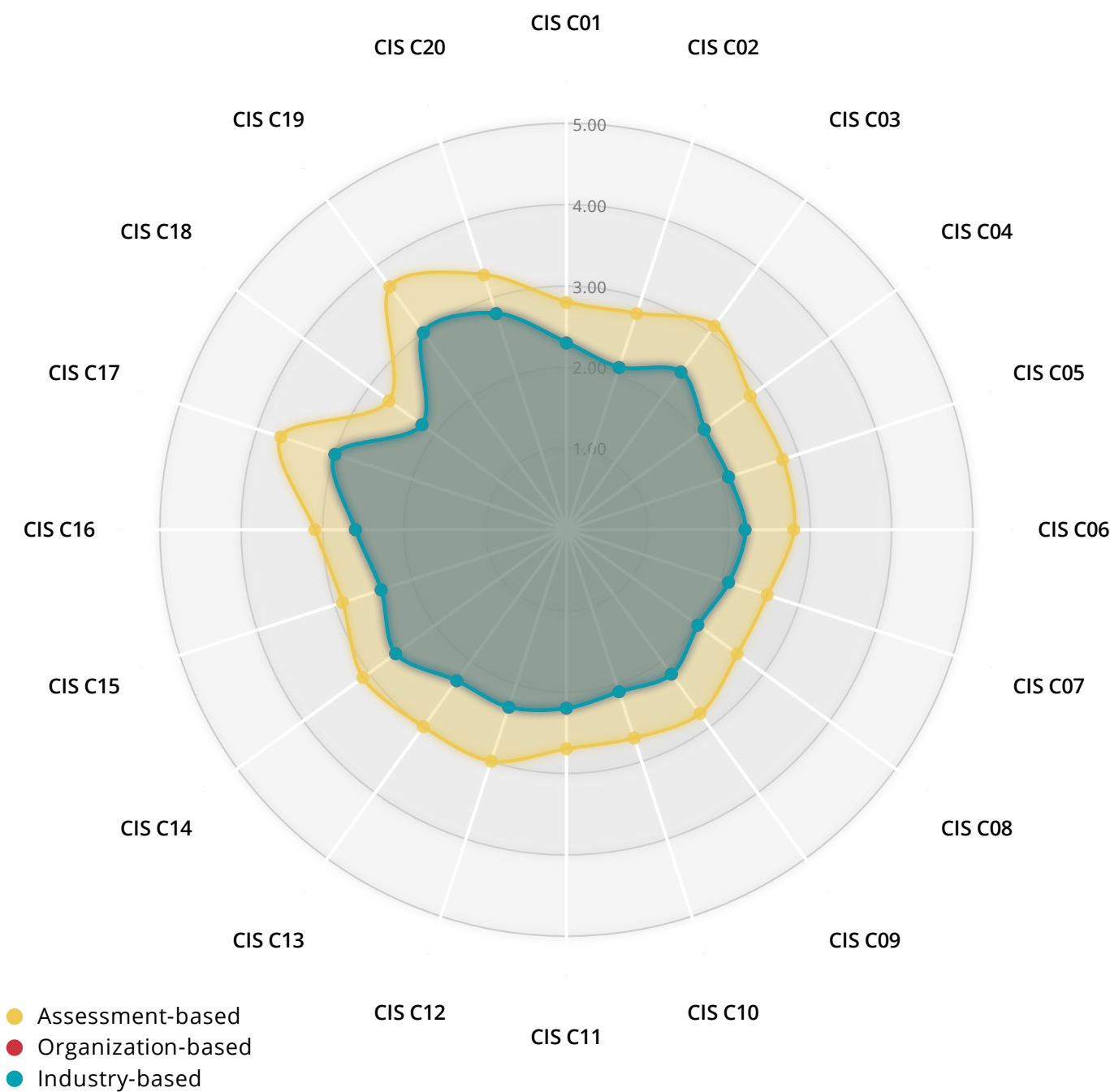


Maturity Level Chart and Graph

3. EXECUTIVE SUMMARY

3.1. Maturity Level

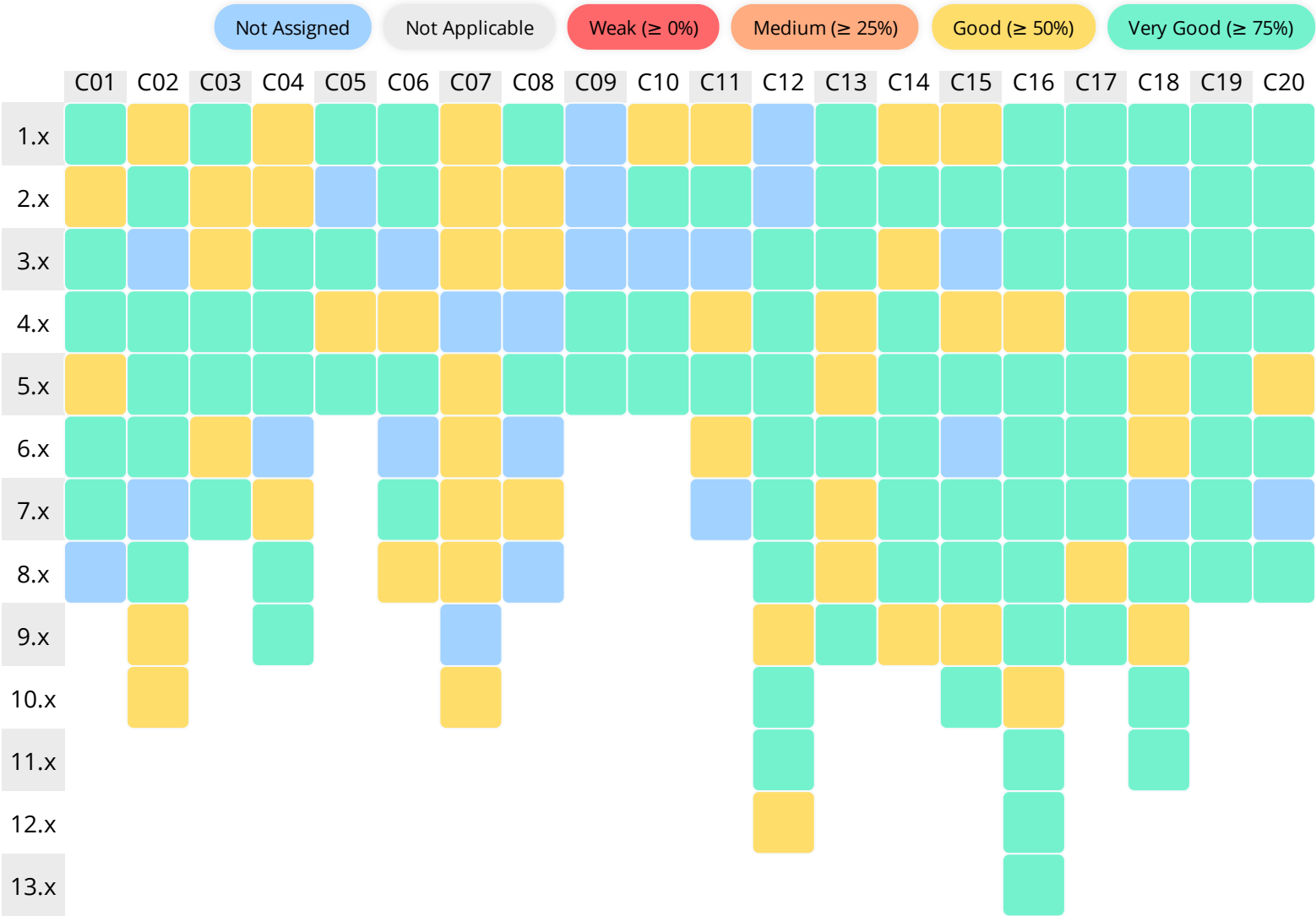
Maturity level, information security with all employees, functioning and assets of an organization It is the level that indicates the information and status of the subject. Determining the maturity level, available taking into account the situation, planning what changes need to be made in the future helps to do. Internationally accepted, used in risk analysis taking into account the standards, the current situation and the targeted situation were compared and the maturity level has been determined. Appropriate action has been taken according to the recommendations in the report. Then the maturity level should be re-evaluated and the point reached should be measured. *ABC Bank LLC* The graph regarding the maturity level of the infrastructure according to CIS 20 Control is given below.



Check Question Based Maturity Level

3.2. CIS 20 Control - Distribution by Category

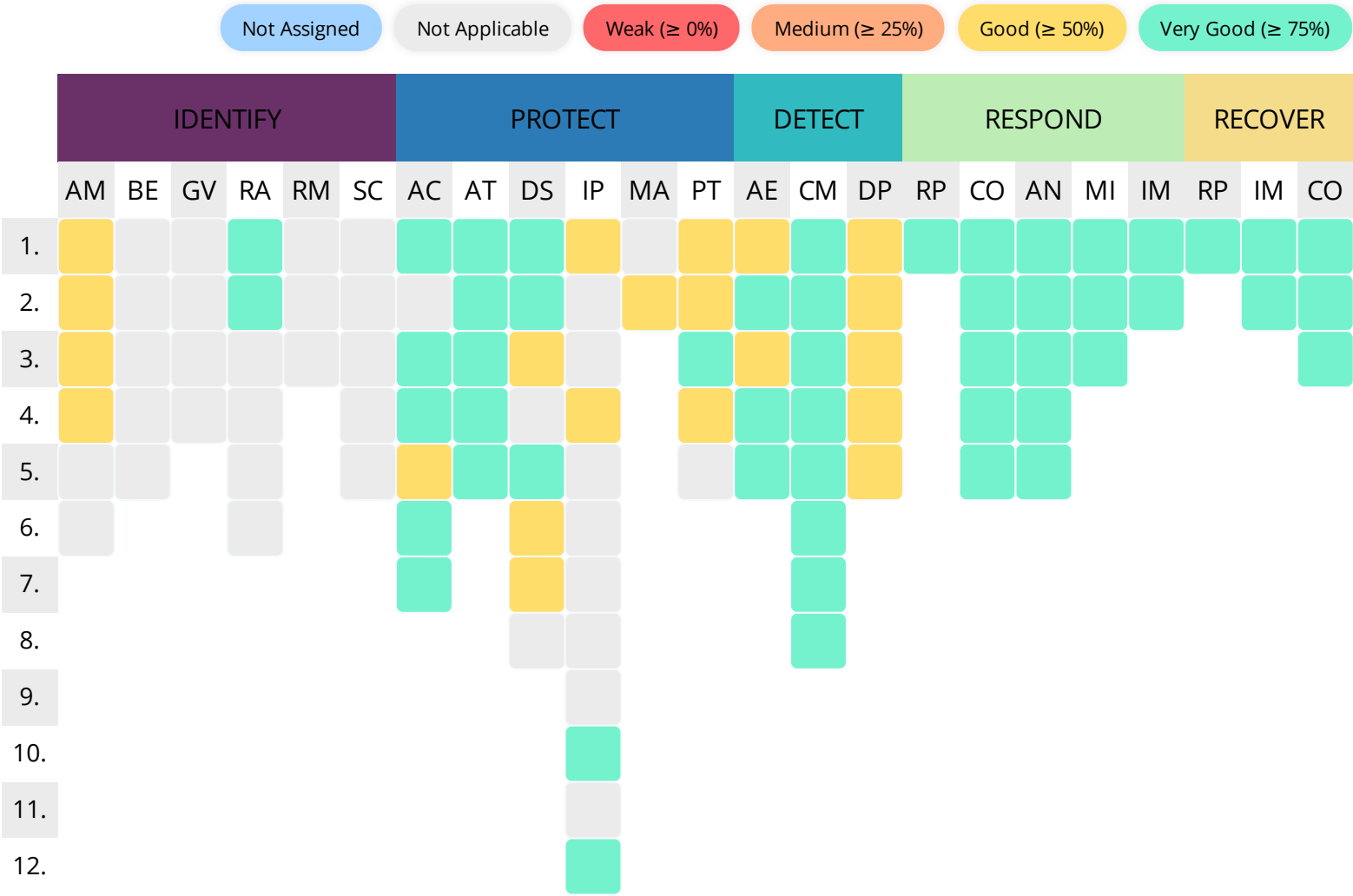
The issues determined as a result of the Cyber Security Maturity Assessment Study are categorized according to CIS 20 Controls and the numerical distribution is shown in the graph below.



State Temperature Map Chart by Categories

3.3. NIST Control - Distribution by Category

The issues determined as a result of the Cyber Security Maturity Assessment Study are categorized according to NIST Controls and the numerical distribution is shown in the graph below.



State Temperature Map Chart by Categories

3.4 Control Categories and Descriptions

CIS C01 : Inventory and Control of Hardware Assets

CIS C02 : Inventory and Control of Software Assets

CIS C03 : Continuous Vulnerability Management

CIS C04 : Controlled Use of Administrative Privileges

CIS C05 : Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

CIS C06 : Maintenance, Monitoring and Analysis of Audit Logs

CIS C07 : Email and Web Browser Protections

CIS C08 : Malware Defenses

CIS C09 : Limitation and Control of Network Ports, Protocols and Services

CIS C10 : Data Recovery Capabilities

CIS C11 : Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

CIS C12 : Boundary Defense

CIS C13 : Data Protection

CIS C14 : Controlled Access Based on the Need to Know

CIS C15 : Wireless Access Control

CIS C16 : Account Monitoring and Control

CIS C17 : Implement a Security Awareness and Training Program

CIS C18 : Application Software Security

CIS C19 : Incident Response and Management

CIS C20 : Penetration Tests and Red Team Exercises

4. CYBER SECURITY MATURITY ASSESSMENT STUDY

This study is based on both NIST Cybersecurity Framework (CSF) and CIS 20 Controls. The expectations of the framework and the current situation of *ABC Bank LLC* have been compared with the expectations of the framework in the form of questions and answers by overlapping each other.

CIS C01 Inventory and Control of Hardware Assets

ISO-27001:2013	A.8.1	A.8.3.2	A.9.3.1	A.10.1.2	A.14.1	A.14.2
----------------	-------	---------	---------	----------	--------	--------

NIST-CSF-1.1	ID.AM-1	ID.AM-3	ID.AM-4	PR.DS-3
--------------	---------	---------	---------	---------

DDO-BG	3.1.1.1	3.1.1.2	3.1.1.3	3.1.1.4	3.1.1.5	3.1.1.6	3.1.1.7	3.1.1.8	3.1.1.9
--------	---------	---------	---------	---------	---------	---------	---------	---------	---------

PCI-DSS-3.2 2.4

BDDK-BS Madde 6

Related Baseline :

- Active Device Discovery System
- Passive Device Discovery System
- Log Management System / SIEM
- Asset Inventory System
- Network Level Authentication (NLA)
- Public Key Infrastructure (PKI)

Status / Score

Completed	%100
Verified	%100
Average Score	%69.53

Status:

- It is understood that the inventory is not up to date.

Steps to be Taken According to the Framework :

- Utilize an Active Discovery Tool
- Use a Passive Asset Discovery Tool
- Use DHCP Logging to Update Asset Inventory
- Maintain Detailed Asset Inventory
- Maintain Asset Inventory Information
- Address Unauthorized Assets
- Deploy Port Level Access Control
- Utilize Client Certificates to Authenticate Hardware Assets

Recommendations :

- Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.
- Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.
- Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.
- Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.
- Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.
- Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.
- Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.
- Use client certificates to authenticate hardware assets connecting to the organization's trusted network.

CIS C02 Inventory and Control of Software Assets

ISO-27001:2013 A.8.1 A12.6.2

NIST-CSF-1.1 ID.AM-2 PR.DS-6

DDO-BG 3.1.2.1 3.1.2.2 3.1.2.3 3.1.2.4 3.1.2.5 3.1.2.6 3.1.2.7




PCI-DSS-3.2 2.4

BDDK-BS Madde 6 Madde 15

Related Baseline :

- Software Application Inventory
- Software Whitelisting System

Status / Score

	Completed	%100
	Verified	%100
	Average Score	%70.63

Status :

Steps to be Taken According to the Framework :

- Maintain Inventory of Authorized Software
- Ensure Software is Supported by Vendor
- Utilize Software Inventory Tools
- Track Software Inventory Information
- Integrate Software and Hardware Asset Inventories
- Address Unapproved Software
- Utilize Application Whitelisting
- Implement Application Whitelisting of Libraries
- Implement Application Whitelisting of Scripts
- Physically or Logically Segregate High Risk Applications

Recommendations :

- Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.
- Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.
- Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.
- The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.
- The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.
- Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.
- Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.
- The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process.
- The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc) are allowed to run on a system.
- Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incur higher risk for the organization.

CIS C03 Continuous Vulnerability Management

ISO-27001:2013 A.14.2.2 A.12.6.2 A.12.6.1 A.12.1.1 A.8.1

NIST-CSF-1.1 ID.RA-1 ID.RA-2 PR.IP-12 DE.CM-8 RS.AN-5 RS.MI-3

DDO-BG 3.1.3.1 3.1.3.2 3.1.3.3 3.1.3.4 3.1.3.5 3.1.3.6 3.1.3.7 3.1.3.8 3.1.3.9 3.1.3.10




PCI-DSS-3.2 6.1 6.2 11.2

BDDK-BS Madde 6 Madde 15 Madde 16

Related Baseline :

- SCAP Based Vulnerability Management System
- Patch Management System

Status / Score

	Completed	%100
	Verified	%100
	Average Score	%77.68

Status :

Steps to be Taken According to the Framework :

- Run Automated Vulnerability Scanning Tools
- Perform Authenticated Vulnerability Scanning
- Protect Dedicated Assessment Accounts
- Deploy Automated Operating System Patch Management Tools
- Deploy Automated Software Patch Management Tools
- Compare Back-to-Back Vulnerability Scans
- Utilize a Risk-Rating Process

Recommendations :

- Utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.
- Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.
- Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.
- Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.
- Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.
- Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.
- Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.

CIS C04 Controlled Use of Administrative Privileges

ISO-27001:2013 A.9.2.3 A.12.4.3 A.9.2

NIST-CSF-1.1 PR.AC-4 PR.AT-2 PR.MA-2 PR.PT-3

DDO-BG 3.1.12.20 3.1.12.5




PCI-DSS-3.2 2.1 7.1 7.2 7.3 8.1 8.2 8.3 8.7

BDDK-BS Madde 11 Madde 38 Madde 39 Madde 40 Madde 41 Madde 42

Related Baseline :

- Privileged Account Management System
- Multi-Factor Authentication System
- Dedicated Administration Systems
- Software Whitelisting System
- Log Management System / SIEM

Status / Score

	Completed	%100
	Verified	%100
	Average Score	%70.83

Status :

- It is understood that the organization do not have any procedure to change default credentials for devices/software.

Steps to be Taken According to the Framework :

- Maintain Inventory of Administrative Accounts
- Change Default Passwords
- Ensure the Use of Dedicated Administrative Accounts
- Use Unique Passwords
- Use Multi-Factor Authentication for All Administrative Access
- Use Dedicated Workstations For All Administrative Tasks
- Limit Access to Scripting Tools
- Log and Alert on Changes to Administrative Group Membership
- Log and Alert on Unsuccessful Administrative Account Login




Recommendations :

- Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.
- Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.
- Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not Internet browsing, email, or similar activities.
- In cases where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords specific to that system.
- Use multi-factor authentication and encrypted channels for all administrative account access.
- Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading email, composing documents, or browsing the Internet.
- Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.
- Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.
- Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers**ISO-27001:2013** **A.6.2** **A.12.2****NIST-CSF-1.1** **PR.IP-1****DDO-BG** **3.3.1.7** **3.3.1.8** **3.3.1.9** **3.3.1.10****PCI-DSS-3.2** **2.2** **2.3** **6.2** **11.5****BDDK-BS** **Madde 15****Related Baseline :**

- System Configuration Baselines & Images
- System Configuration Enforcement System
- SCAP Based Vulnerability Management System

Status / Score

	Completed	%100
	Verified	%100
	Average Score	%70

Status :

- It has been understood that there is no image creation policy related to the systems used in the organization.

Steps to be Taken According to the Framework :

- Establish Secure Configurations
- Maintain Secure Images
- Securely Store Master Images
- Deploy System Configuration Management Tools
- Implement Automated Configuration Monitoring Systems

Recommendations :

- Maintain documented security configuration standards for all authorized operating systems and software.
- Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.
- Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.
- Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.
- Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

CIS C06 Maintenance, Monitoring and Analysis of Audit Logs

ISO-27001:2013 A.12.4 A.16.1.7 A.12.4.4

NIST-CSF-1.1 PR.PT-1 DE.AE-3 DE.DP-1 DE.DP-2 DE.DP-3 DE.DP-4 DE.DP-5

DDO-BG 3.1.8.1 3.1.8.2 3.1.8.3 3.1.8.4 3.1.8.5 3.1.8.6 3.1.8.7 3.1.8.8




PCI-DSS-3.2 10.1 10.2 10.3 10.4 10.5 10.6 10.7 10.8 10.9

BDDK-BS Madde 13 Madde 15 Madde 32 Madde 42 Madde 18

Related Baseline :

- Network Time Protocol (NTP) Systems
- Log Management System / SIEM

Status / Score

	Completed	%100
	Verified	%100
	Average Score	%70.31

Status :

Steps to be Taken According to the Framework :

- Utilize Three Synchronized Time Sources
- Activate Audit Logging
- Enable Detailed Logging
- Ensure Adequate Storage for Logs
- Central Log Management
- Deploy SIEM or Log Analytic Tools
- Regularly Review Logs
- Regularly Tune SIEM

Recommendations :

- Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.
- Ensure that local logging has been enabled on all systems and networking devices.
- Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.
- Ensure that all systems that store logs have adequate storage space for the logs generated.
- Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.
- Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.
- On a regular basis, review logs to identify anomalies or abnormal events.
- On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.

CIS C07 Email and Web Browser Protections

ISO-27001:2013 A.13.2 A.12.2 A.12.1.1 A.14.1.3 A.6.2.2 A.13.2.3

NIST-CSF-1.1 PR.IP-1

DDO-BG 3.1.4.1 3.1.4.2 3.1.4.3 3.1.4.4 3.1.4.5 3.1.4.6 3.1.4.7 3.1.4.8 3.1.4.9 3.1.4.10

3.1.4.11 3.1.4.12 3.1.4.13 3.1.4.14 3.1.4.15 3.1.4.16 3.1.4.17 3.1.4.18 3.1.4.19




PCI-DSS-3.2 2.2 2.3 6.2 11.5

BDDK-BS Madde 14 Madde 16 Madde 15 Madde 9 Madde 29

Related Baseline :

- Software Whitelisting System
- System Configuration Enforcement System
- Network URL Filtering System
- Log Management System / SIEM
- DNS Domain Filtering System
- Anti-Spam Gateway

Status / Score

	Completed	%100
	Verified	%100
	Average Score	%64.38

Status :

Steps to be Taken According to the Framework :

- Ensure Use of Only Fully Supported Browsers and Email Clients
- Disable Unnecessary or Unauthorized Browser or Email Client Plugins
- Limit Use of Scripting Languages in Web Browsers and Email Clients
- Maintain and Enforce Network-Based URL Filters
- Subscribe to URL-Categorization Service
- Log all URL Requests
- Use of DNS Filtering Services
- Implement DMARC and Enable Receiver- Side Verification
- Block Unnecessary File Types
- Sandbox All Email Attachments

Recommendations :

- Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.
- Uninstall or disable any unauthorized browser or email client plugins or add-on applications.
- Ensure that only authorized scripting languages are able to run in all web browsers and email clients.
- Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.
- Subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.
- Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.
- Use Domain Name System (DNS) filtering services to help block access to known malicious domains.
- To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards.
- Block all email attachments entering the organization's email gateway if the file types are unnecessary for the organization's business.
- Use sandboxing to analyze and block inbound email attachments with malicious behavior.

ISO-27001:2013

A.12.2

A.12.4

NIST-CSF-1.1

PR.PT-2

DE.CM-4

DE.CM-5

DDO-BG

3.1.5.1

3.1.5.2

3.1.5.3

3.1.5.4

3.1.5.5

3.1.5.6

3.1.5.7

3.1.5.8

PCI-DSS-3.2

5.1

5.2

5.3

5.4




BDDK-BS

Madde 15

Related Baseline :

- Endpoint Protection System
- System Configuration Enforcement System
- DNS Domain Filtering System
- Log Management System / SIEM

Status / Score

	Completed	%100
	Verified	%100
	Average Score	%65.63

Status :**Steps to be Taken According to the Framework :**

- Utilize Centrally Managed Anti-Malware Software
- Ensure Anti-Malware Software and Signatures are Updated
- Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies
- Configure Anti-Malware Scanning of Removable Devices
- Configure Devices to Not Auto-Run Content
- Centralize Anti-Malware Logging
- Enable DNS Query Logging
- Enable Command-Line Audit Logging

Recommendations :

- Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.
- Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.
- Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.
- Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.
- Configure devices to not auto-run content from removable media.
- Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.
- Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.
- Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.

CIS C09 Limitation and Control of Network Ports, Protocols and Services

ISO-27001:2013 A.13.1 A.12.5 A.14.2.2

NIST-CSF-1.1 PR.AC-5 DE.AE-1

DDO-BG 3.1.6.1 3.1.6.2 3.1.6.3 3.1.6.5




PCI-DSS-3.2 1.4

BDDK-BS Madde 14 Madde 15

Related Baseline :

- SCAP Based Vulnerability Management System
- Host Based Firewall
- Application Aware Firewall

Status / Score

	Completed	%100
	Verified	%100
	Average Score	%68.75

Status :

Steps to be Taken According to the Framework :

- Associate Active Ports, Services and Protocols to Asset Inventory
- Ensure Only Approved Ports, Protocols and Services Are Running
- Perform Regular Automated Port Scans
- Apply Host-Based Firewalls or Port Filtering
- Implement Application Firewalls

Recommendations :

- Associate active ports, services and protocols to the hardware assets in the asset inventory.
- Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system.
- Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.
- Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
- Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.

CIS C10 Data Recovery Capabilities

ISO-27001:2013 A.12.3

NIST-CSF-1.1 PR.IP-4

DDO-BG 3.1.13.1 3.1.13.2 3.1.13.3 3.1.13.4




PCI-DSS-3.2 4.3 9.5 9.6 9.7

BDDK-BS Madde 27 Madde 28

Related Baseline :

- Backup / Recovery System

Status / Score

	Completed	%100
	Verified	%100
	Average Score	%67.5

Status :

- It has been understood that recovery process is not in a regular base.

Steps to be Taken According to the Framework :

- Ensure Regular Automated Backups
- Perform Complete System Backups
- Test Data on Backup Media
- Protect Backups
- Ensure All Backups Have at Least One Offline Backup Destination

Recommendations :

- Ensure that all system data is automatically backed up on a regular basis.
- Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.
- Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.
- Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.
- Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.

CIS C11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

ISO-27001:2013 A.14.2.5 A.14.2 A.12.6.2 A.12.2.1 A.9.1 A.9.2 A.12.5.1 A.12.5 A.12.4.1
A.12.1.3 A.10.1 A.13.1

NIST-CSF-1.1 PR.AC-5 PR.IP-1 PR.PT-4

DDO-BG 3.2.5.1 3.2.5.2 3.2.5.3 3.2.5.4 3.2.5.5 3.2.5.6 3.2.5.7 3.2.5.8 3.2.5.9 3.2.5.10
3.2.5.11 3.1.6.6




PCI-DSS-3.2 1.1 1.2 2.2 6.2

BDDK-BS Madde 15 Madde 26 Madde 28 Madde 11 Madde 34 Madde 38 Madde 39
Madde 40 Madde 41 Madde 42 Madde 14

Related Baseline :

- Network Device Management System
- Multi-Factor Authentication System
- Dedicated Administration Systems

Status / Score

	Completed	%100
	Verified	%100
	Average Score	%67.86

Status :

Steps to be Taken According to the Framework :

- Maintain Standard Security Configurations for Network Devices
- Document Traffic Configuration Rules
- Use Automated Tools to Verify Standard Device Configurations and Detect Changes
- Install the Latest Stable Version of Any Security-Related Updates on All Network Devices
- Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
- Use Dedicated Workstations For All Network Administrative Tasks
- Manage Network Infrastructure Through a Dedicated Network

Recommendations :

- Maintain documented security configuration standards for all authorized network devices.
- All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.
- Compare all network device configurations against approved security configurations defined for each network device in use and alert when any deviations are discovered.
- Install the latest stable version of any security-related updates on all network devices.
- Manage all network devices using multi-factor authentication and encrypted sessions.
- Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading email, composing documents, or surfing the Internet.
- Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

CIS C12 Boundary Defense

ISO-27001:2013 A.13.1.1

NIST-CSF-1.1 PR.AC-3 PR.AC-5 PR.MA-2 DE.AE-1

DDO-BG 3.1.6.18




PCI-DSS-3.2 1.1 1.2 1.3 8.3 10.9 11.4

BDDK-BS Madde 14

Related Baseline :

- Network Firewall / Access Control System
- System Configuration Enforcement System
- Network Packet Capture System
- Network Based Intrusion Detection System (NIDS)
- Network Based Intrusion Prevention System (IPS)
- Network Device Management System
- Multi-Factor Authentication System

Status / Score

	Completed	%100
	Verified	%100
	Average Score	%75.52

Status :

- It has been understood that there is no inventory for network boundary devices.

Steps to be Taken According to the Framework :

- Maintain an Inventory of Network Boundaries
- Scan for Unauthorized Connections across Trusted Network Boundaries
- Deny Communications with Known Malicious IP Addresses
- Deny Communication over Unauthorized Ports
- Configure Monitoring Systems to Record Network Packets
- Deploy Network-Based IDS Sensors
- Deploy Network-Based Intrusion Prevention Systems
- Deploy NetFlow Collection on Networking Boundary Devices
- Deploy Application Layer Filtering Proxy Server
- Decrypt Network Traffic at Proxy
- Require All Remote Logins to Use Multi-Factor Authentication
- Manage All Devices Remotely Logging into Internal Network

Recommendations :

- Maintain an up-to-date inventory of all of the organization's network boundaries.
- Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.
- Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries.
- Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.
- Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.
- Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.
- Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.
- Enable the collection of NetFlow and logging data on all network boundary devices.
- Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.
- Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.
- Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.
- Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.

ISO-27001:2013 A.8.2 A.15.1 A.8.1 A.8.3.2 A.15.2 A.8.3.1 A.13.1 A.8.3

NIST-CSF-1.1 PR.AC-5 PR.DS-2 PR.DS-5 PR.PT-2

DDO-BG 3.1.7.1 3.1.7.2 3.1.7.3 3.1.7.4 3.1.7.5 3.1.7.6 3.1.7.7 3.1.7.8 3.1.7.9 3.1.7.10




PCI-DSS-3.2 3.6 4.1 4.2 4.3

BDDK-BS Madde 5 Madde 6 Madde 29 Madde 9 Madde 15 Madde 14

Related Baseline :

- Data Inventory / Classification System
- Network Based Data Loss Prevention (DLP) System
- Network Firewall / Access Control System
- Whole Disk Encryption System
- Endpoint Protection System

Status / Score

	Completed	%100
	Verified	%100
	Average Score	%75

Status :**Steps to be Taken According to the Framework :**

- Maintain an Inventory of Sensitive Information
- Remove Sensitive Data or Systems Not Regularly Accessed by Organization
- Monitor and Block Unauthorized Network Traffic
- Only Allow Access to Authorized Cloud Storage or Email Providers
- Monitor and Detect Any Unauthorized Use of Encryption
- Encrypt Mobile Device Data
- Manage USB Devices
- Manage System's External Removable Media's Read/Write Configurations
- Encrypt Data on USB Storage Devices

Recommendations :

- Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider.
- Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.
- Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.
- Only allow access to authorized cloud storage or email providers.
- Monitor all traffic leaving the organization and detect any unauthorized use of encryption.
- Utilize approved cryptographic mechanisms to protect enterprise data stored on all mobile devices.
- If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.
- Configure systems not to write data to external removable media, if there is no business need for supporting such devices.
- If USB storage devices are required, all data stored on such devices must be encrypted while at rest.

CIS C14 Controlled Access Based on the Need to Know

ISO-27001:2013 A.6.1.2 A.9.2.6 A.14.1.3 A.9.2 A.12.7 A.12.4 A.9.1 A.9.4

NIST-CSF-1.1 PR.AC-4 PR.AC-5 PR.DS-1 PR.DS-2 PR.PT-2 PR.PT-3

DDO-BG 3.2.3.1 3.2.3.2 3.2.3.4 3.2.3.5




PCI-DSS-3.2 1.3 1.4 4.3 7.1 7.2 7.3 8.7

BDDK-BS Madde 30 Madde 31 Madde 11 Madde 42

Related Baseline :

- Network Firewall / Access Control System
- System Configuration Enforcement System
- Data Inventory / Classification System
- Host Based Data Loss Prevention (DLP) System
- Log Management System / SIEM

Status / Score

	Completed	%100
	Verified	%100
	Average Score	%77.78

Status :

Steps to be Taken According to the Framework :

- Segment the Network Based on Sensitivity
- nable Firewall Filtering Between VLANs
- Disable Workstation-to-Workstation Communication
- Encrypt All Sensitive Information in Transit
- Utilize an Active Discovery Tool to Identify Sensitive Data
- Protect Information through Access Control Lists
- Enforce Access Control to Data through Automated Tools
- Encrypt Sensitive Information at Rest
- Enforce Detail Logging for Access or Changes to Sensitive Data

Recommendations :

- Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).
- Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities
- Disable all workstation-to-workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as private VLANs or micro segmentation.
- Encrypt all sensitive information in transit.
- Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider, and update the organization's sensitive information inventory.
- Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities
- Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when the data is copied off a system.
- Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.
- Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

CIS C15 Wireless Access Control

ISO-27001:2013 A.13.1 A.10.1

NIST-CSF-1.1

DDO-BG 3.1.6.24 3.1.6.25 3.1.6.27 3.1.6.34 3.1.6.35




PCI-DSS-3.2 4.3 11.1

BDDK-BS Madde 14

Related Baseline :

- Network Device Management System
- SCAP Based Vulnerability Management System
- Wireless Intrusion Detection System (WIDS)
- System Configuration Enforcement System

Status / Score

	Completed	%100
	Verified	%100
	Average Score	%71.88

Status :

- It is understood that there is no inventory of wireless devices.

Steps to be Taken According to the Framework :

- Maintain an Inventory of Authorized Wireless Access Points
- Detect Wireless Access Points Connected to the Wired Network
- Use a Wireless Intrusion Detection System
- Disable Wireless Access on Devices if Not Required
- Limit Wireless Access on Client Devices
- Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients
- Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data
- Use Wireless Authentication Protocols that Require Mutual, Multi-Factor Authentication
- Disable Wireless Peripheral Access to Devices
- Create Separate Wireless Network for Personal and Untrusted Devices

Recommendations :

- Maintain an inventory of authorized wireless access points connected to the wired network.
- Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.
- Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.
- Disable wireless access on devices that do not have a business purpose for wireless access.
- Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.
- Disable peer-to-peer (ad hoc) wireless network capabilities on wireless clients.
- Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.
- Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS) that requires mutual, multi-factor authentication.
- Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.
- Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly

CIS C16 Account Monitoring and Control

ISO-27001:2013 A.9.1.1 A.9.2 A.9.4.2 A.6.2 A.9.2.3 A.12.2.1 A.8.1 A.9.2.4 A.9.4.3

NIST-CSF-1.1 PR.AC-1 PR.AC-4 PR.AC-6 PR.AC-7 PR.PT-3

DDO-BG 3.1.12.1 3.1.12.2 3.1.12.3 3.1.12.4 3.1.12.6 3.1.12.7 3.1.12.8 3.1.12.9 3.1.12.10

3.1.12.11 3.1.12.12 3.1.12.13 3.1.12.14 3.1.12.15 3.1.12.16 3.1.12.17 3.1.12.18 3.1.12.19

3.1.12.21




PCI-DSS-3.2 7.1 7.2 7.3 8.7 8.8

BDDK-BS Madde 11 Madde 38 Madde 39 Madde 40 Madde 41 Madde 42

Related Baseline :

- Identity & Access Management System
- Multi-Factor Authentication System
- Log Management System / SIEM

Status / Score

	Completed	%100
	Verified	%100
	Average Score	%78.37

Status :

Steps to be Taken According to the Framework :

- Maintain an Inventory of Authentication Systems
- Configure Centralized Point of Authentication
- Require Multi-Factor Authentication
- Encrypt or Hash all Authentication Credentials
- Encrypt Transmittal of Username and Authentication Credentials
- Maintain an Inventory of Accounts
- Establish Process for Revoking Access
- Disable Any Unassociated Accounts
- Disable Dormant Accounts
- Ensure All Accounts Have An Expiration Date
- Lock Workstation Sessions After Inactivity
- Monitor Attempts to Access Deactivated Accounts
- Alert on Account Login Behavior Deviation

Recommendations :

- Maintain an inventory of each of the organization's authentication systems, including those located on-site or at a remote service provider.
- Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.
- Require multi-factor authentication for all user accounts, on all systems, whether managed on-site or by a third-party provider.
- Encrypt or hash with a salt all authentication credentials when stored.
- Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.
- Maintain an inventory of all accounts organized by authentication system.
- Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.
- Disable any account that cannot be associated with a business process or business owner.
- Automatically disable dormant accounts after a set period of inactivity.
- Ensure that all accounts have an expiration date that is monitored and enforced.
- Automatically lock workstation sessions after a standard period of inactivity.
- Monitor attempts to access deactivated accounts through audit logging.
- Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.

CIS C17 Implement a Security Awareness and Training Program

ISO-27001:2013 A.7.3 A.7.2.2 A.16.1

NIST-CSF-1.1 PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5

DDO-BG 3.5.2.1 3.5.2.2 3.5.2.3


PCI-DSS-3.2 12.6

BDDK-BS Madde 8 Madde 14 Madde 19

Related Baseline :

- Training / Awareness Education Plans

Status / Score

	Completed	%100
	Verified	%100
	Average Score	%92.36

Status :

Steps to be Taken According to the Framework :

- Perform a Skills Gap Analysis
- Deliver Training to Fill the Skills Gap
- Implement a Security Awareness Program
- Update Awareness Content Frequently
- Train Workforce on Secure Authentication
- Train Workforce on Identifying Social Engineering Attacks
- Train Workforce on Sensitive Data Handling
- Train Workforce on Causes of Unintentional Data Exposure
- Train Workforce Members on Identifying and Reporting Incidents

Recommendations :

- Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.
- Deliver training to address the skills gap identified to positively impact workforce members' security behavior.
- Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner
- Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.
- Train workforce members on the importance of enabling and utilizing secure authentication.
- Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls.
- Train workforce members on how to identify and properly store, transfer, archive and destroy sensitive information.
- Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.
- Train workforce members to be able to identify the most common indicators of an incident and be able to report such an incident.

CIS C18 Application Software Security

ISO-27001:2013 A.14.1 A.14.3

NIST-CSF-1.1 PR.DS-7

DDO-BG 3.2.6.1 3.2.6.2 3.2.6.3 3.2.6.4 3.2.6.5 3.2.6.6 3.2.6.7 3.2.6.8




PCI-DSS-3.2 6.3 6.5a 6.5b 6.6 6.7

BDDK-BS Madde 22 Madde 23

Related Baseline :

- Secure Coding Standards
- Training / Awareness Education Plans
- Software Vulnerability Scanning Tool
- Web Application Firewall (WAF)
- System Configuration Enforcement System

Status / Score

	Completed	%100
	Verified	%100
	Average Score	%67.61

Status :

Steps to be Taken According to the Framework :

- Establish Secure Coding Practices
- Ensure Explicit Error Checking is Performed for All In-House Developed Software
- Verify That Acquired Software is Still Supported
- Only Use Up-to-Date And Trusted Third-Party Components
- Use Only Standardized and Extensively Reviewed Encryption Algorithms
- Ensure Software Development Personnel are Trained in Secure Coding
- Apply Static and Dynamic Code Analysis Tools
- Establish a Process to Accept and Address Reports of Software Vulnerabilities
- Separate Production and Non-Production Systems
- Deploy Web Application Firewalls
- Use Standard Hardening Configuration Templates for Databases

Recommendations :

- Establish secure coding practices appropriate to the programming language and development environment being used.
- For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.
- Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.
- Only use up-to-date and trusted third-party components for the software developed by the organization.
- Use only standardized, currently accepted, and extensively reviewed encryption algorithms.
- Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.
- Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.
- Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.
- Maintain separate environments for production and non-production systems. Developers should not have unmonitored access to production environments.
- Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.
- For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.

CIS C19 Incident Response and Management

ISO-27001:2013 A.16.1 A.7.2

NIST-CSF-1.1 PR.IP-10 DE.AE-2 DE.AE-4 DE.AE-5 DE.CM-1 DE.CM-2 DE.CM-3 DE.CM-4
DE.CM-5 DE.CM-6 DE.CM-7 RS.RP-1 RS.CO-1 RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5 RS.AN-1
RS.AN-2 RS.AN-3 RS.AN-4 RS.MI-1 RS.MI-2 RS.IM-1 RS.IM-2 RC.RP-1 RC.IM-1 RC.IM-2
RC.CO-1 RC.CO-2 RC.CO-3

DDO-BG 3.1.10.1 3.1.10.2 3.1.10.3 3.1.10.4 3.1.10.5 3.1.10.6 3.1.10.7 3.1.10.8




PCI-DSS-3.2 12.10

BDDK-BS Madde 18

Related Baseline :

- Incident Management Plans

Status / Score

	Completed	%100
	Verified	%100
	Average Score	%92.19

Status :

Steps to be Taken According to the Framework :

- Document Incident Response Procedures
- Assign Job Titles and Duties for Incident Response
- Designate Management Personnel to Support Incident Handling
- Devise Organization-wide Standards for Reporting Incidents
- Maintain Contact Information For Reporting Security Incidents
- Publish Information Regarding Reporting Computer Anomalies and Incidents
- Conduct Periodic Incident Scenario Sessions for Personnel
- Create Incident Scoring and Prioritization Schema




Recommendations :

- Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management.
- Assign job titles and duties for handling computer and network incidents to specific individuals and ensure tracking and documentation throughout the incident through resolution.
- Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.
- Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.
- Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and Information Sharing and Analysis Center (ISAC) partners.
- Publish information for all workforce members, regarding reporting computer anomalies and incidents, to the incident handling team. Such information should be included in routine employee awareness activities.
- Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real-world threats. Exercises should test communication channels, decision making, and incident responder's technical capabilities using tools and data available to them.
- Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.

Related Baseline :

- Penetration Testing Plans

Status / Score

	Completed	%100
	Verified	%100
	Average Score	%82.81

Status :

Steps to be Taken According to the Framework :

- Establish a Penetration Testing Program
- Conduct Regular External and Internal Penetration Tests
- Perform Periodic Red Team Exercises
- Include Tests for Presence of Unprotected System Information and Artifacts
- Create a Test Bed for Elements Not Typically Tested in Production
- Use Vulnerability Scanning and Penetration Testing Tools in Concert
- Ensure Results from Penetration Test are Documented Using Open, Machine-readable Standards
- Control and Monitor Accounts Associated with Penetration Testing

Recommendations :

- Establish a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks.
- Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.
- Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.
- Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, emails or documents containing passwords or other information critical to system operation.
- Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.
- Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.
- Wherever possible, ensure that Red Team results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.
- Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.

5. CONCLUSION

Information security management is a process that must be kept alive and open to continuous improvement by adapting to changes. Risk analysis and risk processing processes specified in this report should be applied periodically. In this way, it is determined how much the applied controls achieve their purpose. In addition, since information technologies are changing very rapidly, it is important to include assets that are newly included in the corporate system in risk management. In addition to these, the business objectives of the institution, the way it does business and the issues it attaches importance to may change over time. All these changes cause changes in vulnerabilities, threats, and risks. Continuous operation of the risk management cycle will ensure that the risks posed by all these changes are recognized and addressed by management.

A successful and effective information security management; The support and ownership of the senior management, the awareness of all employees through various trainings and managerial arrangements, the determination of priority risks for the organization and the appropriate solutions to reduce these risks, the application of these solutions in the most appropriate way to the institution, periodic auditing of these applications and continuous improvement by making the necessary improvements as a result of these. can be provided as a result of change.


As in many subjects, the most critical success factor in information security is conscious and knowledgeable people. The ultimate goal in information security management should be to transform information security into a corporate culture over time. A successful and long-term information security management; awareness of information security can be provided by people through training, information and awareness. In addition to risk-reducing technological or process solutions, it is also important to enforce policies, procedures and rules that will regulate the way the organization does business.

The measures to be implemented to improve the capability of critical cyber security controls, in 3 different order of priority;

RECOMMENDED IN SHORT TERM

- Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.
- Maintain an inventory of authorized wireless access points connected to the wired network.

RECOMMENDED IN MIDDLE TERM

- Ensure that both the hardware and software inventory are kept up-to-date.
 - Ensure that the organization have controls to change the default credentials.
 - Maintain an up-to-date inventory of all of the organization's network boundaries.
- 

RECOMMENDED IN LONG TERM

- Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards.



CYBER SCORE

Contact

Address: İcerenkoy Mah. Topcu Ibrahim Sk. AND Plaza No: 8-10D
Atasehir / Istanbul

Phone: +90 216 474 00 38

Fax: +90 216 474 93 86

E-Mail: info@cyberscorecard.io

* This report was generated automatically on : *date* . If you think there is a mistake and / or missing, please contact the technical team.