**Introduction:**

This Tier-1 questionnaire collects first-level information for conducting a Cyber Security Resilience Examination (CSRE) within your institution. The questionnaire is divided into two sheets which are the General Information Sheet (GIS) and the Detail Information Sheet (DIS). The GIS enable the examiner to estimate the size of your company/institution to determine which controls are required for an adequate protection of your information assets against Cyber Security risks. The DIS includes those 3 domain areas as adopted by the Bank from the Center for Internet Security (CIS) IS Audit/Assurance Program for Cyber Security Resilience. The collected information from the DIS, helps the examiner primarily assess the existence and secondly to some extend the effectiveness of those 20 Cyber Security Controls (CSC) from the domain areas as recommended by CIS. These controls are listed in the first and their requirements in the second column of the Tier-1 detail sheet. The examination objective is to identify and report to management significant weaknesses and vulnerabilities found within the institution’s internal control system for information security and to bring some recommendations to reduce risks the institution is exposed to. Additional explanation is given to some requests in the last column. The same column must be used to fill the answers or provide the information as requested, by replacing the information recorded in the last column. Some questions or requests may be easily answered or filled with “Yes”, “No” or “Not Applicable”.

**Tier-1 General Information Sheet (GIS):**

|  | **Requested information:** | **Explanation/information to be provided:** |
| --- | --- | --- |
| General information. | | |
| **General Information** | G.1 Indicate the number of employees working into the company/institution and the number of personnel working into your IT-Department? | Number of employees:  Number of IT-staff: |
| G.2 Indicate the number of desktops/laptops make available to all employees for resource services purposes? | Number of desktops:  Number of laptops: |
| G.3 Provide a copy of the LAN/WAN infrastructure of the institution/company. |  |
| G.4 Indicate the number of servers (application, database, proxies), routers, firewalls, switches and other network nodes providing network and resource services to personnel? | Servers:  Routers:  Firewalls:  Switches:  Other network nodes: |
| G.5 Indicate if any web-service and/or e-mail  service is make available to internal employees or  the public? |  |
|  | G.6 Indicate the number of applications supporting the key function of your business? | Number of applications: |
|  | G.7 Indicate as per last year the total amount  invested into network infrastructure, hardware and software? |  |

**Tier-1 Detail Information Sheet (DIS):**

| **Controls:** | **Requested information:** | | | **Explanation/information to be provided:** |
| --- | --- | --- | --- | --- |
| Domain Area A: System. | | | | |
| **CSC 1: Inventory of Authorized and**  **Unauthorized Devices.** | 1.1 Provide any governance arrangements, procedures and tools employed by your institution to manage device inventory. | | |  |
| 1.2 Indicate if assets inventory take place periodically and provide frequency and most recent list of these assets. | | |  |
| 1.3 Provide a list of names with existing procedures and their date of approval by management for the procurement, acquisition, setup and deployment, decommissioned and removed of systems from the network. Submit copies of procedures if available. | | |  |
| 1.4 Indicate if your institution blocks or have controls in place to detect immediately when new devices are connected to the network. | | |  |
| 1.5 Indicate whether encryption is applied for internal network traffic. | | |  |
| 1.6a Does your institution use client certificates to validate and authenticate systems prior to connecting to the private network.  1.6b Are switches employed to allow only authorized devices to connect to the network and hereafter reconcile with the assets inventory. | | |  |
| **CSC 2: Inventory of Authorized and Unauthorized Software.** | 2.1 Provide most recent list of authorized software and their version for each type of system (including servers, workstations and laptops). Secondly, provide procedures/arrangements made to bring changes on the list. | | |  |
| 2.2 Indicate if the institution has a tool or controls to whitelist software which is allowed to run on servers, workstations and laptops. If available, provide further information on the tool or the controls in place. | | |  |
| 2.3 Indicate whether the institutions has an automated tool or controls for the inventory of software installed on computer systems. If available, provide further information on the tool or the controls in place. | | |  |
| 2.4 Indicate if some security high risk devices are connected to/or separated from the institution’s main network. | | | These are devices such as back door routers and WIFI, which pose a security risk to the network, when connected to the network. |
|  |  | | |  |
| **CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops and Servers.** | 3.1 Provide if available policies and procedures for the configuration/hardening of operating systems and application software, servers, laptops and desktops that protects these systems against known attacks or vulnerabilities. | | |  |
| 3.2 Indicate whether your institution is using secure images to build all new systems that are deployed within the institution. | | |  |
| 3.3 Describe controls that guarantee secure storage of the master images. | | |  |
| 3.4 Provide if available, the institution’s policies and procedures for remote access to server, laptops, desktops and other computer systems. | | |  |
| 3.5 Indicate whether your institutions has tools to check the integrity of critical systems files (including configuration, libraries, and executables files) from being altered. | | |  |
| 3.6 Indicate whether your institution has deployed an automated configuration monitoring system that detects and reports unauthorized configurations to critical systems e.g. their listening ports, new administrative user changes to group and local policies objects. | | |  |
| 3.7 Has your institution deployed an automated system configuration management tool to enforce the mandatory security configuration settings on systems? | | |  |
| **CSC4: Continuous Vulnerability Assessment and Remediation** | 4.1 Indicate whether your institution has deployed vulnerability scanning tools to evaluate the security settings of systems. | | |  |
| 4.2 Are event logs correlated with scanning tools information? | | | Correlating event logs with vulnerability scanning tools information is a control to determine the effectiveness of the vulnerability scanning activities |
| 4.3 Indicate authentication controls and permissions granted on remote systems or the local host for running scanning tools? | | | Scanning tools should be run by authorized personnel with specific account’s permissions. |
| 4.4 Are vulnerabilities scanning tools upgraded regularly and periodically verified on their effectiveness? | | |  |
| 4.5 Does your institution apply automated tools for (timely) patching of operating and application system’s software? | | |  |
| 4.6 Indicate whether logs of scanning activities are reviewed and for which purpose. | | | The objective of reviewing logs of scanning activities is to determine the legitimacy of the scan. |
| 4.7 Indicate follow-up activities conducted by your institution on vulnerabilities discovered or controls established, to assure that these are timely resolved or remediated. | | |  |
|  | 4.8 Does your institution applied a rating system for prioritizing vulnerabilities found? | | |  |
| CSC 5: Controlled use of Administrative Privileges. | 5.1 Describe existing controls (e.g. PAN Privilege Access System) for the assignment and monitoring of activities of accounts with administrative privileges granted to administrators, users and applications. | | |  |
| 5.2 Indicate whether accounts with administrative privileges on domain controllers and local systems are periodically reconciled against the inventory list approved by the organization. | | |  |
| 5.3 Are controls in place for changing password default settings to the corporate settings for administrative-level accounts on all new devices?. | | |  |
| 5.4 Indicate whether changes to administrators account on domain servers and local systems are automatically monitored through alerts? | | |  |
| |  | | --- | | 5.5 Indicate whether failed login to administrators  account on domain servers and local systems are  automatically monitored through alerts. | | | |  |
| 5.6 Indicate whether privilege accounts on critical systems require a two- or multifactor authentication for access. | | |  |
| 5.7 Indicate whether the password policy for access to critical systems privilege accounts enforce strong or complex passwords and provide password policy settings. | | |  |
| 5.8 Indicate whether or not systems are configured using administrative privilege accounts for direct remote access. | | | |  | | --- | | Administrators should be required to access a system using non-administrative accounts that is fully logged. Then, once signed on, to the network the administrator should use its’ administrative account. | |
| 5.9 Indicate whether for the maintenance of elevated or highly secured systems such as firewalls, IPS and IDS, dedicated machines are established, which are separated from the primary network. | | |  |
| **CSC 6: Maintenance, Monitoring and Analysis of Audit Logs** | 6.1 Indicate whether internal system’s time is synchronized with external time zone servers. | | |  |
| 6.2 Provide the institution’s policy for audit log settings and standards. | | | Logs must include a date- and timestamp, source addresses, destination addresses and various other useful elements of each packet and/or transaction and should record logs in a standardized format. |
| 6.3 Indicate existing controls for the management of storage space on systems recording logs information. | | |  |
| 6.4 Indicate whether audit logs report are generated and independently reviewed by e.g. security officers. | | |  |
| 6.5 Indicate whether network boundary devices such as firewalls and IPS/IDS are configured to log all in- and outbound traffic. | | |  |
| 6.6 Indicate whether any SIEM (Security Information and Event Management) tool is used to help monitor and detect suspicious or unusual security/system events. | | | SIEM are tools that generally collect and analyze log data. |
| **CSC 7: Email and Web Browser Protection** | 7.1 Indicate how and if software installed for web browsing on clients, servers and gateways systems are kept up to date and effective enough against malicious software attacks. | | |  |
| 7.2 Provide the institution’s policy for the installation of add on and plugins on end-user devices such as laptops, workstations and mobile devices, web browsers and email clients. | | | Plugins or add-on are scripting languages used to design certain application tasks. |
| 7.3 Provide the institution’s policy for the use of  scripting languages in web browsers and email clients. | | |  |
| 7.4 Indicate whether all web traffic or URL requests from servers, laptops, workstation and mobile devices are logged/recorded and monitored by a proxy server. | | |  |
| 7.5 Indicate whether two separate browsers are configured, one that enable the use of plugins and scripting languages for such functionality, and a second one where these scripts are disabled. | | |  |
| 7.6 Provide information on any network-based URL-filtering employed by your institution that limit access to system’s ability to connect to uncategorized websites. | | |  |
| 7.7 Indicate or describe any control or tools used by your institution such as SPF (Sender Policy Framework, DKIM (Domain Keys Identified Mail) and DMARC (Domain Message Authentication Reporting & Conformance) to reduce the risk of email spoofing. | | |  |
| 7.8 Indicate if firewall rules direct emails to email gateways and describe complementary controls/tools employed by your institution for the filtering of malicious emails, attachments and web traffic. | | |  |
| **CSC 8: Malware Defenses** | 8.1 Are workstations, servers, laptops and mobile devices equipped with most recent and effective anti-malware tool? Describe how these systems are kept up running with the most up to date versions. | | |  |
| 8.2 Are malware detection events monitored and sent automatically to a central server for analysis purposes? | | |  |
| 8.3 Describe controls for the protection of the internal network against external devices plugged into the network or removable media running on external or internal devices? | | |  |
| 8.4 Indicate if any anti-exploitation tool such as DEP (Data Execution Prevention) and ASLR (Address Space Layout Randomization) are used to reduce the probability to exploit existing vulnerabilities on systems? | | |  |
| 8.5 Indicate if any network based anti-malware tool is employed to identify executables in network traffic? | | |  |
| 8.6 Has your institutions enabled query logging on the DNS to detect hostnames lookup for known malicious domains? | | |  |
| **CSC 9: Limitation and Control of Network Ports, Protocols and Services** | 9.1 Are policies established and enforced for hardening systems allowing these to run with ports, protocols and services that are only needed by the business? | | |  |
| 9.2 Indicate which (critical) systems apply host based firewalls or port-filtering tools and provide the applicable rules for the allowed ports/service traffic. | | |  |
| 9.3 Are key (critical) servers scanned on a regular basis for unnecessary services running and open ports? | | |  |
| 9.4 Provide all those servers made available to untrusted networks like the Internet. | | |  |
| 9.5 Indicate whether critical services like Web, file, mail, DNS and Dbase servers are operated on separated physical or logical hosts. | | |  |
| 9.6 Are application firewalls installed in front of any of those servers listed in 9.2 till 9.5, that block unauthorized services going to these servers?. | | |  |
| **CSC 10: Data Recovery Capability** | 10.1 Provide the institution’s back up policy and procedure for e.g. operating and application systems and data. | | |  |
| 10.2 Indicate whether regular restoration tests are conducted to guarantee that back up is properly working. Provide evidence of the last test done. | | |  |
| 10.3 Indicate security applied to protect backup data, either stored in a remote location or via cloud services. | | |  |
| 10.4 Indicate if critical systems are backed-up on at least two different destinations/locations? | | |  |
|  | | | | |
| Domain Area B : Network. | | | | |
| **CSC11: Secure Configurations for Network Devices such as Firewalls, Routers and Switches** | 11.1 Does the institution has standard secure configuration for each type of network device like firewalls, routers and switches? Are these standards approved by management and provide these if available. | | |  |
| 11.2 Are changes made to the baseline standard security configuration documented and recorded in a configuration management system? | | |  |
| 11.3 Describe existing controls that independently detect changes made to the baseline standard security configuration. | | |  |
| 11.4 Indicate if two-factor authentication is required for access to and enforced on critical network devices and if the session is encrypted? | | |  |
| 11.5 Is the security of all critical network devices patched regularly with the latest updates? Describe control procedure for the updates | | |  |
| 11.6 Are dedicated machines available to network engineers for administrative tasks on critical network devices and describe the security configurations of these machines? | | |  |
| 11.7 Provide entire network infrastructure and indicate if machines managing this network infrastructure are separated from the business network through e.g. VLANS or other connectivity. | | |  |
| **CSC12: Boundary Defense** | 12.1 Indicate if the internal network is segmented from any untrusted network (like the Internet) using firewalls and proxy’s that look for black-listed IP-addresses or to allow only white-listed sites. | | |  |
| 12.2 Are IDS configured in the Demilitarized Zone (DMZ) that looks for attacks against the protected network and hence filter packet header information for transmission to a SIEM? | | | A DMZ is configured between the internal network and the untrusted network (like the Internet). The purpose of a DMZ is to add an additional layer of security to an organization's [local area network](https://en.wikipedia.org/wiki/Local_area_network) (LAN). An external [network node](https://en.wikipedia.org/wiki/Network_node) can access only those resources which are exposed in the DMZ. |
| 12.3 Are network-based IDS equipped with the use of signatures, network behavior analysis and other mechanisms? Are these systems periodically tested on their capability to detect compromised attacks? | | |  |
| 12.4 Are network-based IPS devices deployed to complement IDS by blocking known bad signatures? | | |  |
| 12.5 Indicate whether all outbound traffic must traverse through a proxy server with capabilities to e.g. decrypt network traffic, log TCP-sessions and block certain domain names and URL’s | | |  |
| 12.6 Indicate whether single or two-factor authentication is employed for remote logins to internal systems using VPN, dial-up and other forms of access? | | |  |
| 12.7 Provide if available the security standards, policy and controls for the configuration of remote access devices from internal users and business partners | | |  |
| 12.8 Indicate controls executed by the institution to prevent/detect back-channel devices. | | | |  | | --- | | Back-channel devices are connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms. | |
| 12.9 Indicate any other tool deployed into the DMZ to detect anomalous activity | | |  |
| 12.10 Indicate whether firewalls are configured to identify TCP-sessions that last longer than normal. | | |  |
| **CSC13: Data Protection** | 13.1 Has your institution define a data classification policy?. | | |  |
| 13.2 Are standards and policy employed for the protection of data on mobile devices and when these are stored and transferred either internally or externally? | | |  |
| 13.3 Is there any tool used to identify exfiltration attempts of sensitive information like personally identifiable information? | | |  |
| 13.4 Does your institution conduct periodical scans or controls on server to detect if sensitive data is encrypted or present on these systems in clear text? | | |  |
| 13.5 Are policies available to protect systems against writing data to USB tokens or hard drives? | | |  |
| 13.6 Is there any tool used (Data Loss Prevention DLP-solutions) to monitor and control the flow of internal data within the network? | | |  |
| 13.7 Indicate whether controls are in place to detect if unauthorized encrypted data is leaving the organization and so bypassing security devices? | | |  |
| 13.8 Is access blocked to known file transfer and email exfiltration websites | | |  |
| 13.9 Is any host-based DLP tool used that enforce ACL’s (Access Control List) when (critical) data is copied from a server? | | |  |
|  |  | | |  |
|  |  | | |  |
| Domain Area C: Application. | | | | |
| **CSC14: Controlled Access Based on the Need to Know** | | 14.1 Indicate whether the network is segmented (VLANS) through e.g. firewalls based on the classification or protection level of the information stored on the servers. Indicate whether for segmentation purposes, data is at least categorized into public and private data. |  | |
| 14.2 Indicate whether sensitive information travelling on less trusted network is encrypted or not? | A less trusted network is operated by a third party, for which no assurance exist that encryption is applied on the data transmitted on this network. | |
| 14.3 Indicate if network switches are configured to limit workstations on a network to communicate with other devices on the subnet? |  | |
| 14.4 Are all information stored on systems protected through file systems, network share, application and database specific ACL’s? |  | |
| 14.5 Are sensitive/critical information stored encrypted? And is a secondary authentication mechanism, not integrated into the operating system, required for access to this information |  | |
| 14.6 Indicate whether your policy require audit logging for access to non-public data and secondly a special authentication for sensitive data? |  | |
| 14.7 Are data sets or systems which are not regularly used, removed from the corporate network and stored on a stand-alone system? |  | |
| **CSC15: Wireless Access Control** | | 15.1 Are wireless devices connected to the network? Are the configuration and security profile of these devices authorized? |  | |
| 15.2 Are commercial wireless scanning tools employed to detect wireless access points connected to the network? |  | |
| 15.3 Does your institution employ WIDS (wireless intrusion detection systems) and is traffic to the wired network monitored? |  | |
| 15.4 Provide the institution’s security policy and configuration for granting clients’ machines wireless access |  | |
| 15.5 Indicate encryption standard used for wireless traffic and if WPA2 (Wi-Fi Protected Access 2) is used? |  | |
| 15.6 Indicate whether the institution’s wireless networks use EAP (Extensible Authentication Protocol or TLS (Transport Layer Security) for authentication? If not, indicate any other protocol used. |  | |
| 15.7 Indicate if peer-to peer wireless connections are allowed on the clients’ machines? |  | |
| 15.8 Indicate if any wireless peripheral access of devices (such as Bluetooth) is enabled? |  | |
| 15.9 Is there a separate VLAN created for BYOD (Bring Your Own Device) systems and is access from this VLAN treated as untrusted and filtered/audited accordingly? |  | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CSC16: Account Monitoring and Control** | 16.1 Provide list with active **system** accounts (including non-personalized accounts) for all operating system platforms and indicate whether these accounts are periodically traced back to authorized users of the systems. |  | | |
| 16.2 Indicate whether active system accounts have an expiration date. If so indicate the policy for expiration length and if these accounts are periodically recertified for their continued use. |  | | |
| 16.3 Provide UAM (User Account Management) internal policies and procedures for e.g. removing/revoking system access from end-user accounts. | |  | |
| 16.4 Indicate whether operating system access activities are logged on all system’s platforms and that a tool is used to analyze the logged data? | |  | |
| 16.5 Indicate whether access to unattended critical workstations is protected using screen locks. | |  | |
| 16.6 Provide the institution’s policy for dormant accounts. | | |  |
| 16.7 Provide the institution’s policy for failed login attempts. | |  | |
| 16.8 Is access to deactivated accounts monitored through audit logging? | |  | |
| 16.9 Are accounts, network and security devices configured through a centralized point of authentication like AD and LDAP? Provide password settings policy for these accounts and network/security devices? | |  | |
| 16.10 Are user’s typical account’s usage normal time-of-day profile defined and monitored? | |  | |
| 16.11 Is multi-factor authentication required for users’ account’s access to sensitive data or systems? | |  | |
| 16.12 Indicate password policy set for access to systems. | |  | |
| 16.13 Provide the institution’s policy for transmitting usernames and credentials over the network channels. | |  | |
| 16.14 Are authentication files encrypted or hashed and is access to these files protected via root or privilege permissions? | |  | |
|  | |  | |
|  |  | |  | |
|  |  | |  | |
| **CSC17: Security Skills Assessment And Appropriate Training to Fill Gaps** | 17.1 Indicate whether your institution has performed a gap analysis to identify training needed for implementation of security controls. | |  | |
| 17.2 Provide training program and security awareness training given to staff during the last 2 years. | |  | |
| 17.3 Indicate whether key staff has been trained on common intrusion attack techniques and data privacy and other regulations, during the last 2 years. | |  | |
| 17.4 Indicate whether your institution conduct test to determine the awareness level of personnel. | | Such tests include e.g. general phishing (suspicious emails with a link to an external site that records all employees who click on the link), piggybacking and social engineering. | |
| 17.5 Indicate whether training is categorized and focus first on mission critical jobs. | | Mission critical jobs include e.g.  1) System and network penetration testers  2) Application penetration testers  3) Security monitoring and event analysts  4) Incident responders in-depth  5) Counter-intelligence/insider threat analysts  6) Risk assessment engineers  7) Secure coders and code reviewers  8) Security engineers/architecture and design  9) Security engineers/operations  10) Advanced forensics analysts | |
| **CSC18: Application Software Security** | 18.1 Describe existing controls that help detect non-supported version or outdated application software running on systems. | |  | |
| 18.2 Indicate if a web- or host application firewall is configured to inspect all traffic going to that web (or non-web) application. | |  | |
| 18.3 Provide evidence e.g. test scripts and results which proof that critical in-house developed critical web-/non web applications, have been tested on error checking for all input data e.g. size and data type. | |  | |
| 18.4 Indicate whether in-house developed and third party web applications are scanned regularly on commonly known security weaknesses? Provide if available results/reports of these scans. | |  | |
| 18.5 Indicate whether in-house developed and third party web applications are tested on inappropriate system error messages displayed to end-users? Provide if available test scripts and results. | |  | |
| 18.6 Indicate if separation exist between production and non-production environment and between developers, operators and end-users. Provide evidence that proof this. | |  | |
| 18.7 Provide policy and/or standard configuration templates established for the hardening of applications using databases. | |  | |
| 18.8 Provide training received by software development personnel during the last 3 years. | |  | |
| 18.9 Provide if available controls and procedures for the deployment of internal developed software to the production environment. | |  | |
| **CSC19: Incident Response And Management** | 19.1 Provide the institution’s incident response policies and procedures. | |  | |
| 19.2 Are job titles and duties assigned to specific individuals for computer and network incidents? | |  | |
| 19.3 Does procedures clearly define management personnel who is responsible for key decision in case of incidents? Provide names of the management personnel involved. | |  | |
| 19.4 Provide standards and policies established for deadlines and other requirements (including root cause analysis) for internal reporting of incidents or anomalous events by system administrators and other personnel to the incident handling team. | |  | |
| 19.5 Provide list with names of third party contacts, which need to be informed in case of an incident. | |  | |
| 19.6 Indicate when and how employees and other contractors are informed upon reported incidents. | |  | |
| 19.7 Are members of the incident handling team regularly trained upon currents threats and risks? | |  | |
| **CSC20: Penetration Tests And Red Team Exercises** | 20.1 Indicate if any internal or external penetration test has been done during the last 2 years. Provide a copy of the reports if available. | |  | |
| 20.2 Indicate controls applied to users’ and/or system accounts used for conducting penetration tests. | |  | |
| 20.3 Does the incident responds team conduct routine exercises to stop, respond quickly and effectively on attacks? | |  | |
| 20.4 Are tests conducted to identify if useful information such as network diagrams, configuration files, penetration test report etc. etc. are left behind to attackers? | |  | |
| 20.5 Describe the institution’s penetration test objective, strategy and target assets for the last test done. | |  | |
| 20.6 Indicate whether latest penetration tests are done in concert with vulnerability scanning assessments. | |  | |
| 20.7 Indicate whether the results of the incident respond team are documented. | |  | |
| 20.8 Are non-tested elements (e.g. supervisory control and other control systems) of the production environment simulated in a test bed for penetration testing purposes? | |  | |