ETSI TR 103 305-1 V2.1.1

CYBER;

Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

ETSI TR 103 305-1
Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

Published August 2016 - https://www.etsi.org/deliver/etsi_tr/103300_103399/10330501/03.01.01_60/tr_10330501v030101p.pdf

Describes a specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of cyber attacks

- Developed and maintained by the Center for Internet Security (CIS)

The Controls are designed to:

- Block the initial compromise of systems
- Address detecting already-compromised machines and preventing or disrupting attackers' follow-on actions
- Reduce the initial attack surface by hardening device configurations
- Identify compromised machines to address long-term threats inside an organization's network
- Disrupting attackers' command-and-control of implanted malicious code
- Establish an adaptive, continuous defence and response capability that can be maintained and improved

ETSI TR 103 305-1 Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

- The five critical tenets of an effective cyber defence system as reflected in the Critical Security Controls are:
  - Offense informs defence: Use knowledge of actual attacks that have compromised systems to provide the foundation to continually learn from these events to build effective, practical defences. Include only those controls that can be shown to stop known real-world attacks
  - Prioritization: Invest first in Controls that will provide the greatest risk reduction and protection against the most dangerous threat actors, and that can be feasibly implemented in a computing environment
  - Metrics: Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly
  - Continuous diagnostics and mitigation: Carry out continuous measurement to test and validate the effectiveness of current security measures, and to help drive the priority of next steps
  - Automation: Automate defences so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the Controls and related metrics

ETSI TR 103 305-1
Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

Key Definition:

Critical Security Control (CSC): Specified capabilities that reflect the combined knowledge of actual attacks and effective defences of experts that are maintained by the Center for Internet Security

ETSI TR 103 305-1
Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

Critical Controls

- **CSC 1: Inventory of Authorized and Unauthorized Devices**: *Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access*
- **CSC 2: Inventory of Authorized and Unauthorized Software**: *Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution*
- **CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**: *Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings*
- **CSC 4: Continuous Vulnerability Assessment and Remediation**: *Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers*

ETSI TR 103 305-1
Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

Critical Controls

- **CSC 5: Controlled Use of Administrative Privileges**: *The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications*
- **CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs**: *Collect, manage, and analyze audit logs of events that could help detect, understand or recover from an attack*
- **CSC 7: Email and Web Browser Protections**: *Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems*
- **CSC 8: Malware Defenses**: *Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action*
- **CSC 9: Limitation and Control of Network Ports, Protocols, and Services**: *Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers*

ETSI TR 103 305-1
Critical Security Controls for Effective Cyber Defence;
Part 1: The Critical Security Controls

Critical Controls

- **CSC 10: Data Recovery Capability**: *The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it*
- **CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches**: *Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings*
- **CSC 12: Boundary Defense**: *Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security damaging data*
- **CSC 13: Data Protection**: *The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information*
- **CSC 14: Controlled Access Based on the Need to Know**: *The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g. information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification*

ETSI TR 103 305-1
Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

Critical Controls

- **CSC 15: Wireless Access Control**: *The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANs), access points, and wireless client systems*
- **CSC 16: Account Monitoring and Control**: *Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them*
- **CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps**: *For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs*
- **CSC 18: Application Software Security**: *Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses*

ETSI TR 103 305-1
Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

Critical Controls

- **CSC 19: Incident Response and Management**: *Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g. plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems*
- **CSC 20: Penetration Tests and Red Team Exercises**: *Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker*

CSC 1: Inventory of Authorized and Unauthorized Devices - Controls

Control	Control Description
1.1	Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.
1.2	If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.
1.3	Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.
1.4	Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created should also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data should be identified, regardless of whether they are attached to the organization's network.
1.5	Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x should be tied into the inventory data to determine authorized versus unauthorized systems [i.3].
1.6	Use client certificates to validate and authenticate systems prior to connecting to the private network

ETSI TR 103 305-1
Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 2: Inventory of Authorized and Unauthorized Software - Controls

Control	Control Description
2.1	Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.
2.2	Deploy application whitelisting that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.
2.3	Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. The software inventory systems should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.
2.4	Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment.

CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers - Controls

Control	Control Description
3.1	Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.
3.2	Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the organization's change management processes. Images should be created for workstations, servers, and other system types used by the organization.
3.3	Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.
3.4	Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers - Controls

Control	Control Description
3.5	Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The reporting system should: have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the Su or Sudo command). These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).
3.6	Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system. Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.
3.7	Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows® systems or Puppet for Unix systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis.

ETSI TR 103 305-1
Critical Security Controls for Effective Cyber Defence;
Part 1: The Critical Security Controls

CSC 4: Continuous Vulnerability Assessment and Remediation - Controls

Control	Control Description
4.1	Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).
4.2	Correlate event logs with information from vulnerability scans to fulfil two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools is itself logged. Second, personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.
4.3	Perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative 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. Ensure that only authorized employees have access to the vulnerability management user interface and that roles are applied to each user.
4.4	Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization's vulnerability scanning activities on at least a monthly basis. Alternatively, ensure that the vulnerability scanning tools used are regularly updated with all relevant important security vulnerabilities.

CSC 4: Continuous Vulnerability Assessment and Remediation - Controls

Control	Control Description
4.5	Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.
4.6	Monitor logs associated with any scanning activity and associated administrator accounts to ensure that this activity is limited to the timeframes of legitimate scans
4.7	Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed, either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed, increasing the risk
4.8	Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops). Apply patches for the riskiest vulnerabilities first. A phased rollout can be used to minimize the impact to the organization. Establish expected patching timelines based on the risk rating level

CSC 5: Controlled Use of Administrative Privileges - Controls

Control	Control Description
5.1	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.
5.2	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.
5.3	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.
5.4	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.
5.5	Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account.
5.6	Use multi-factor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.

ETSI TR 103 305-1 Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 5: Controlled Use of Administrative Privileges - Controls

Control	Control Description
5.7	Where multi-factor authentication is not supported, user accounts should be required to use long passwords on the system (longer than 14 characters)
5.8	Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/Unix, Run As on Windows®, and other similar facilities for other types of systems
5.9	Administrators should use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine should be isolated from the organization's primary network and not be allowed Internet access. This machine should not be used for reading email, composing documents, or surfing the Internet.

ETSI TR 103 305-1
Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs - Controls

Control	Control Description
6.1	Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.
6.2	Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.
6.3	Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs should be archived and digitally signed on a periodic basis.
6.4	Have security personnel and/or system administrators run biweekly reports that identify anomalies in logs. They should then actively review the anomalies, documenting their findings.
6.5	Configure network boundary devices, including firewalls, network-based IPS, and inbound and outbound proxies, to verbosely log all traffic (both allowed and blocked) arriving at the device.
6.6	Deploy a SIEM (Security Information and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIEM tool, system administrators and security personnel should devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.

ETSI TR 103 305-1 Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 7: Email and Web Browser Protections - Controls

Control	Control Description
7.1	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 provided by the vendor in order to take advantage of the latest security functions and fixes.
7.2	Uninstall or disable any unnecessary or unauthorized browser or email client plugins road-on applications. Each plugin should utilize application / URL whitelisting and only allow the use of the application for pre-approved domains.
7.3	Limit the use of unnecessary scripting languages in all web browsers and email clients. This includes the use of languages such as ActiveX and JavaScript on systems where it is unnecessary to support such capabilities.
7.4	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.
7.5	Deploy two separate browser configurations to each system. One configuration should disable the use of all plugins, unnecessary scripting languages, and generally be configured with limited functionality and be used for general web browsing. The other configuration should allow for more browser functionality but should only be used to access specific websites that require the use of such functionality.

ETSI TR 103 305-1 Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 7: Email and Web Browser Protections - Controls

Control	Control Description
7.6	The organization should maintain and enforce network based URL filters that limit a system's ability to connect to websites not approved by the organization. The organization should subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites should be blocked by default. This filtering should be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.
7.7	To lower the chance of spoofed email messages, implement the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver-side verification in mail servers.
7.8	Scan and block all email attachments entering the organization's email gateway if they contain malicious code or file types that are unnecessary for the organization's business. This scanning should be done before the email is placed in the user's inbox. This includes email content filtering and web content filtering

ETSI TR 103 305-1 Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 8: Malware Defenses - Controls

Control	Control Description
8.1	Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.
8.2	Employ anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update.
8.3	Limit use of external devices to those with an approved, documented business need. Monitor for use and attempted use of external devices. Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e. "thumb drives"), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares. Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted
8.4	Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.
8.5	Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.
8.6	Enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains.

ETSI TR 103 305-1
Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 9: Limitation and Control of Network Ports, Protocols, and Services - Controls

Control	Control Description
9.1	Ensure that only ports, protocols, and services with validated business needs are running on each system.
9.2	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.
9.3	Perform automated port scans on a regular basis against all key servers and compare to a known effective baseline. If a change that is not listed on the organization's approved baseline is discovered, an alert should be generated and reviewed.
9.4	Verify any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, move it to an internal VLAN and give it a private address.
9.5	Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers.
9.6	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized services or traffic should be blocked and an alert generated.

ETSI TR 103 305-1 Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 10: Data Recovery Capability - Controls

Control	Control Description
10.1	Ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive information. To help ensure the ability to rapidly restore a system from backup, the operating system, application software, and data on a machine should each be included in the overall backup procedure. These three components of a system do not have to be included in the same backup file or use the same backup software. There should be multiple backups over time, so that in the event of malware infection, restoration can be from a version that is believed to predate the original infection. All backup policies should be compliant with any regulatory or official requirements.
10.2	Test data on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.
10.3	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.
10.4	Ensure that key systems have at least one backup destination that is not continuously addressable through operating system calls. This will mitigate the risk of attacks like CryptoLocker which seek to encrypt or damage data on all addressable data shares, including backup destinations

ETSI TR 103 305-1 Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches – Controls

Control	Control Description
11.1	Compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization. The security configuration of such devices should be documented, reviewed, and approved by an organization change control board. Any deviations from the standard configuration or updates to the standard configuration should be documented and approved in a change control system.
11.2	All new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPS, should be documented and recorded in a configuration management system, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need.
11.3	Use automated tools to verify standard device configurations and detect changes. All alterations to such files should be logged and automatically reported to security personnel.
11.4	Manage network devices using two-factor authentication and encrypted sessions.
11.5	Install the latest stable version of any security-related updates on all network devices.
11.6	Network engineers should use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine should be isolated from the organization's primary network and not be allowed Internet access. This machine should not be used for reading email, composing documents, or surfing the Internet.
11.7	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.

ETSI TR 103 305-1
Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 12: Boundary Defense – Controls

Control	Control Description
12.1	Deny communications with (or limit data flow to) known malicious IP addresses (blacklists), or limit access only to trusted sites (whitelists). Tests can be periodically carried out by sending packets from bogon source IP addresses (non-routable or otherwise unused IP addresses) into the network to verify that they are not transmitted through network perimeters. Lists of bogon addresses are publicly available on the Internet from various sources, and indicate a series of IP addresses that should not be used for legitimate traffic traversing the Internet.
12.2	On DMZ networks, configure monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border. This traffic should be sent to a properly configured Security Information Event Management (SIEM) or log analytics system so that events can be correlated from all devices on the network.
12.3	Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic.
12.4	Network-based IPS devices should be deployed to complement IDS by blocking known bad signatures or the behavior of potential attacks. As attacks become automated, methods such as IDS typically delay the amount of time it takes for someone to react to an attack. A properly configured network-based IPS can provide automation to block bad traffic. When evaluating network-based IPS products, include those using techniques other than signature-based detection (such as virtual machine or sandbox based approaches) for consideration.

CSC 12: Boundary Defense – Controls

Control	Control Description
12.5	Design and implement network perimeters so that all outgoing network traffic to the Internet should pass through at least one application layer filtering proxy server. The proxy should support decrypting network traffic, logging individual TCP sessions, blocking specific URLs, domain names, and IP addresses to implement a black list, and applying whitelists of allowed sites that can be accessed through the proxy while blocking all other sites. Organizations should force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter.
12.6	Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.
12.7	All enterprise devices remotely logging into the internal network should be managed by the enterprise, with remote control of their configuration, installed software, and patch levels. For third-party devices (e.g. subcontractors/vendors), publish minimum security standards for access to the enterprise network and perform a security scan before allowing access.
12.8	Periodically scan for back-channel 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	Deploy NetFlow collection and analysis to DMZ network flows to detect anomalous activity
12.10	To help identify covert channels exfiltrating data through a firewall, configure the built-in firewall session tracking mechanisms included in many commercial firewalls to identify TCP sessions that last an unusually long time for the given organization and firewall device, alerting personnel about the source and destination addresses associated with these long sessions.

ETSI TR 103 305-1
Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 13: Data Protection – Controls

Control	Control Description
13.1	Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls.
13.2	Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.
13.3	Deploy an automated tool on network perimeters that monitors for sensitive information (e.g. personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.
13.4	Conduct periodic scans of server machines using automated tools to determine whether sensitive data (e.g. personally identifiable information, health, credit card, or classified information) is present on the system in clear text. These tools, which search for patterns that indicate the presence of sensitive information, can help identify if a business or technical process is leaving behind or otherwise leaking sensitive information.
13.5	If there is no business need for supporting such devices, configure systems so that they will not write data to USB tokens or USB hard drives. If such devices are required, enterprise software should be used that can configure systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and that can automatically encrypt all data placed on such devices. An inventory of all authorized devices should be maintained.
13.6	Use network-based DLP solutions to monitor and control the flow of data within the network. Any anomalies that exceed the normal traffic patterns should be noted and appropriate action taken to address them.

ETSI TR 103 305-1
Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 13: Data Protection– Controls

Control	Control Description
13.7	Monitor all traffic leaving the organization and detect any unauthorized use of encryption. Attackers often use an encrypted channel to bypass network security devices. Therefore it is essential that organizations be able to detect rogue connections, terminate the connection, and remediate the infected system.
13.8	Block access to known file transfer and email exfiltration websites.
13.9	Use host-based data loss prevention (DLP) to enforce ACLs even when data is copied off a server. In most organizations, access to the data is controlled by ACLs that are implemented on the server. Once the data have been copied to a desktop system, the ACLs are no longer enforced and the users can send the data to whomever they want.

ETSI TR 103 305-1 Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 14: Controlled Access Based on the Need to Know – Controls

Control	Control Description
14.1	Segment the network based on the label or classification level of the information stored on the servers. Locate all sensitive information on separated VLANs with firewall filtering to ensure that only authorized individuals are only able to communicate with systems necessary to fulfil their specific responsibilities.
14.2	All communication of sensitive information over less-trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted.
14.3	All network switches will enable Private Virtual Local Area Networks (VLANs) for segmented workstation networks to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attackers ability to laterally move to compromise neighboring systems.
14.4	All information stored on systems should be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principal that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.
14.5	Sensitive information stored on systems should be encrypted at rest and require a secondary authentication mechanism, not integrated into the operating system, in order to access the information.
14.6	Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data.
14.7	Archived data sets or systems not regularly accessed by the organization should be removed from the organization's network. These systems should 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.

ETSI TR 103 305-1 Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 15: Wireless Access Control – Controls

Control	Control Description
15.1	Ensure that each wireless device connected to the network matches an authorized configuration and security profile, with a documented owner of the connection and a defined business need. Organizations should deny access to those wireless devices that do not have such a configuration and profile.
15.2	Configure network vulnerability scanning tools to detect wireless access points connected to the wired network. Identified devices should be reconciled against a list of authorized wireless access points. Unauthorized (i.e. rogue) access points should be deactivated.
15.3	Use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromises. In addition to WIDS, all wireless traffic should be monitored by WIDS as traffic passes into the wired network.
15.4	Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks. For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (basic input/output system or extensible firmware interface).
15.5	Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection.
15.6	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which provide credential protection and mutual authentication.

ETSI TR 103 305-1 Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 15: Wireless Access Control – Controls

Control	Control Description
15.7	Disable peer-to-peer wireless network capabilities on wireless clients
15.8	Disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need
15.9	Create separate virtual local area networks (VLANs) for BYOD systems or other untrusted devices. Internet access from this VLAN should go through at least the same border as corporate traffic. Enterprise access from this VLAN should be treated as untrusted and filtered and audited accordingly.

ETSI TR 103 305-1
Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 16: Account Monitoring and Control – Controls

Control	Control Description
16.1	Review all system accounts and disable any account that cannot be associated with a business process and owner.
16.2	Ensure that all accounts have an expiration date that is monitored and enforced.
16.3	Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails.
16.4	Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.
16.5	Configure screen locks on systems to limit access to unattended workstations.
16.6	Monitor account usage to determine dormant accounts, notifying the user or user’s manager. Disable such accounts if not needed, or document and monitor exceptions (e.g. vendor maintenance accounts needed for system recovery or continuity operations). Require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators should then disable accounts that are not assigned to valid workforce members.
16.7	Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.
16.8	Monitor attempts to access deactivated accounts through audit logging.
16.9	Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

ETSI TR 103 305-1 Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 16: Account Monitoring and Control – Controls

Control	Control Description
16.10	Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works.
16.11	Require multi-factor authentication for all user accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using smart cards, certificates, One Time Password (OTP) tokens or biometrics.
16.3	Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails.
16.12	Where multi-factor authentication is not supported, user accounts should be required to use long passwords on the system (longer than 14 characters).
16.13	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels
16.14	Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps – Controls

Control	**Control Description**
17.1	Perform gap analysis to see which skills employees need to implement the other Controls, and which behaviors employees are not adhering to, using this information to build a baseline training and awareness roadmap for all employees.
17.2	Deliver training to fill the skills gap. If possible, use more senior staff to deliver the training. A second option is to have outside teachers provide training onsite so the examples used will be directly relevant. If there are small numbers of people to train, use training conferences or online training to fill the gaps.
17.3	Implement a security awareness program that:1) focuses on the methods commonly used in intrusions that can be blocked through individual action;2) is delivered in short online modules convenient for employees;3) is updated frequently (at least annually) to represent the latest attack techniques;4) is mandated for completion by all employees at least annually;5) is reliably monitored for employee completion; and6) includes the senior leadership team's personal messaging, involvement in training, and accountability through performance metrics.
17.4	Validate and improve awareness levels through periodic tests to see whether employees will click on a link from suspicious email or provide sensitive information on the telephone without following appropriate procedures for authenticating a caller; targeted training should be provided to those who fall victim to the exercise.
17.5	Use security skills assessments for each of the mission-critical roles to identify skills gaps. Use hands-on, real-world examples to measure mastery. If there are no such assessments, use one of the available online competitions that simulate real-world scenarios for each of the identified jobs in order to measure mastery of skills mastery.

ETSI TR 103 305-1 Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 18: Application Software Security – Controls

Control	Control Description
18.1	For all acquired application software, check that the version used is still supported by the vendor. If not, update to the most current version and install all relevant patches and vendor security recommendations.
18.2	Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks, including but not limited to cross-site scripting, SQL injection, command injection, and directory traversal 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.
18.3	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.
18.4	Test in-house-developed and third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to deployment, whenever updates are made to the application, and on a regular recurring basis. In particular, input validation and output encoding routines of application software should be reviewed and tested.
18.5	Do not display system error messages to end-users (output sanitization)
18.6	Maintain separate environments for production and nonproduction systems. Developers should not typically have unmonitored access to production environments.

ETSI TR 103 305-1
Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 18: Application Software Security – Controls

Control	Control Description
18.7	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.
18.8	Ensure that all software development personnel receive training in writing secure code for their specific development environment.
18.9	For in-house developed applications, ensure that development artifacts (sample data and scripts; unused libraries, components, debug code; or tools) are not included in the deployed software, or accessible in the production environment.

ETSI TR 103 305-1 Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 19: Incident Response and Management – Controls

Control	Control Description
19.1	Ensure that there are written incident response procedures that include a definition of personnel roles for handling incidents. The procedures should define the phases of incident handling.
19.2	Assign job titles and duties for handling computer and network incidents to specific individuals.
19.3	Define management personnel who will support the incident handling process by acting in key decision-making roles.
19.4	Devise organization-wide standards for the time required for system administrators and other personnel 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. This reporting should also include notifying the appropriate Community Emergency Response Team in accordance with all legal or regulatory requirements for involving that organization in computer incidents.
19.5	Assemble and maintain information on third-party contact information to be used to report a security incident (e.g. maintain an email address of security@organization.com or have a web page http://organization.com/security).
19.6	Publish information for all personnel, including employees and contractors, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.
19.7	Conduct periodic incident scenario sessions for personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team.

ETSI TR 103 305-1 Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 20: Penetration Tests and Red Team Exercises – Controls

Control	Control Description
20.1	Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Penetration testing should occur from outside the network perimeter (i.e. the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e. on the internal network) to simulate both outsider and insider attacks.
20.2	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.
20.3	Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.
20.4	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.
20.5	Plan clear goals of the penetration test itself with blended attacks in mind, identifying the goal machine or target asset. Many APT-style attacks deploy multiple vectors-often social engineering combined with web or network exploitation. Red Team manual or automated testing that captures pivoted and multi-vector attacks offers a more realistic assessment of security posture and risk to critical assets.

ETSI TR 103 305-1 Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

CSC 20: Penetration Tests and Red Team Exercises – Controls

Control	Control Description
20.6	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.
20.7	Wherever possible, ensure that Red Teams 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.
20.8	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.

ETSI TR 103 305-1 Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

Attack Types

- Attackers continually scan for new, unprotected systems, including test or experimental systems, and exploit such systems to gain control of them
- Attackers distribute hostile content on Internet-accessible (and sometimes internal) websites that exploit unpatched and improperly secured client software running on victim machines
- Attackers continually scan for vulnerable software and exploit it to gain control of target machines
- Attackers use currently infected or compromised machines to identify and exploit other vulnerable machines across an internal network
- Attackers exploit weak default configurations of systems that are more geared to ease of use than security
- Attackers exploit new vulnerabilities on systems that lack critical patches in organizations that do not know that they are vulnerable because they lack continuous vulnerability assessments and effective remediation
- Attackers compromise target organizations that do not exercise their defenses to determine and continually improve their effectiveness
- Attackers use malicious code to gain and maintain control of target machines, capture sensitive data, and then spread it to other systems, sometimes wielding code that disables or dodges signature-based anti-virus tools

ETSI TR 103 305-1
Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

Attack Types

- Attackers scan for remotely accessible services on target systems that are often unneeded for business activities, but provide an avenue of attack and compromise of the organization
- Attackers exploit weak application software, particularly web applications, through attack vectors such as SQL injection, cross-site scripting, and similar tools
- Attackers exploit wireless access points to gain entry into a target organization's internal network, and exploit wireless client systems to steal sensitive information
- Attackers exploit users and system administrators via social engineering scams that work because of a lack of security skills and awareness
- Attackers exploit and infiltrate through network devices whose security configuration has been weakened over time by granting, for specific short-term business needs, supposedly temporary exceptions that are never removed
- Attackers trick a user with an administrator-level account into opening a phishing-style email with an attachment or surfing to the attacker's content on an Internet website, allowing the attacker's malicious code or exploit to run on the victim machine with full administrator privileges
- Attackers exploit boundary systems on Internet-accessible DMZ networks, and then pivot to gain deeper access on internal networks

ETSI TR 103 305-1 Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

Attack Types

- Attackers exploit poorly designed network architectures by locating unneeded or unprotected connections, weak filtering, or a lack of separation of important systems or business functions
- Attackers operate undetected for extended periods of time on compromised systems because of a lack of logging and log review
- Attackers gain access to sensitive documents in an organization that does not properly identify and protect sensitive information or separate it from non-sensitive information
- Attackers compromise inactive user accounts left behind by temporary workers, contractors, and former employees, including accounts left behind by the attackers themselves who are former employees
- Attackers escalate their privileges on victim machines by launching password guessing, password cracking, or privilege escalation exploits to gain administrator control of systems, which is then used to propagate to other victim machines across an enterprise
- Attackers gain access to internal enterprise systems and gather and exfiltrate sensitive information without detection by the victim organization
- Attackers compromise systems and alter important data, potentially jeopardizing organizational effectiveness via polluted information
- Attackers operate undiscovered in organizations without effective incident-response capabilities, and when the attackers are discovered, the organizations often cannot properly contain the attack, eradicate the attacker's presence, or recover to a secure production state