Western Balkans Chevening Cybersecurity Alumni

Expanded Self-Assessment Cybersecurity Framework for SMEs

Version 2.2 , September 2024

Aleksandar Acev
Solza Kovachevska

Expanded Self-Assessment Cybersecurity Framework for SMEs

Introduction

The Expanded Self-Assessment Cybersecurity Framework for SMEs (ESACF) aims to integrate the fundamental principles of the NCSC Cyber Essentials with the advanced guidelines of the NIST Cybersecurity Framework (CSF) 2.0. This framework is specifically designed to assist small and medium-sized enterprises (SMEs) in evaluating and enhancing their cybersecurity measures. Each section includes questions that align with both frameworks, offering detailed explanations to help assess current cybersecurity practices and identify areas for improvement. While these measures are comprehensive for SMEs, they are not equivalent to the standards required for Critical Infrastructure or Essential Services, which address different levels of security needs and complexities.

1. NCSC Cyber Essentials

The NCSC Cyber Essentials is a UK government-backed scheme designed to help organisations of all sizes protect themselves against a wide range of the most common cyber attacks. The scheme offers a basic but effective framework to ensure that key areas of cybersecurity are covered.

The main objectives of Cyber Essentials are to help organisations protect Against Common Cyber Threats. The Cyber Essentials scheme focuses on basic technical controls that can significantly reduce the risk of prevalent cyber threats. It helps organisations safeguard their data and systems from common forms of attack, such as phishing, malware, and hacking.

Implement Key Security Measures: Cyber Essentials sets out five key controls that organisations should have in place to protect themselves. These controls are:

- Firewalls and Internet Gateways: To secure internet connections and control incoming and outgoing network traffic.
- Secure Configuration: To ensure that systems are configured securely to reduce vulnerabilities.
- Access Control: To ensure that only authorised individuals have access to systems and data.
- Malware Protection: To protect against viruses, spyware, and other malicious software.
- Patch Management: To keep software and devices up to date with the latest security patches.

The Cyber Essentials scheme includes essential defensive technical controls designed to reduce the risk of successful cyber attacks. Although data backup is not mandatory in Cyber Essentials, as it is not a defensive measure, it is crucial for recovery if an attack occurs. Therefore, while not a technical requirement,

regularly backing up and testing data files is highly recommended. Similarly, asset management is not a specific Cyber Essentials control but is a vital security function. By emphasising asset management within the Cyber Essentials recommendations, the scheme highlights its importance for maintaining robust cybersecurity practices.

By adhering to Cyber Essentials, organisations can improve their overall cyber hygiene. This involves adopting basic practices and measures that can prevent security breaches and enhance the resilience of their IT infrastructure. Achieving Cyber Essentials certification demonstrates a commitment to cybersecurity. This can enhance an organisation's reputation, build customer trust, and provide a competitive edge in the marketplace.

While Cyber Essentials is not a legal requirement, it can support compliance with other regulatory and contractual requirements. Organisations that achieve Cyber Essentials certification are often better prepared to meet broader cybersecurity standards and regulations.

More information about this framework is available at: https://www.ncsc.gov.uk/cyberessentials

2. NIST Cybersecurity Framework (CSF) 2.0

The NIST Cybersecurity Framework (CSF) is a comprehensive and flexible framework developed by the National Institute of Standards and Technology (NIST) in the United States. It provides a policy framework of computer security guidance for how private sector organisations can assess and improve their ability to prevent, detect, and respond to cyber attacks. This framework focuses on technical and organisational controls that can support an organisation’s efforts to reduce the risk of prevalent cyber threats. The CSF is widely recognized and adopted globally for its effectiveness in managing and reducing cybersecurity risk.

The framework is built around five core functions:

- Identify (ID): This function assists in developing an organisational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- Protect (PR): This function outlines appropriate safeguards to ensure the delivery of critical infrastructure services.
- Detect (DE): This function defines the activities necessary to identify the occurrence of a cybersecurity event.
- Respond (RS): This function includes appropriate activities to take action regarding a detected cybersecurity incident.
- Recover (RC): This function identifies appropriate activities to maintain plans for resilience and to restore capabilities or services that were impaired due to a cybersecurity incident.

The NIST CSF provides a structured approach to managing cybersecurity risks, covering all aspects from identification and protection to detection, response, and recovery. The framework is designed to be flexible and can be tailored to the specific needs and risk environments of different organisations, regardless of size or industry. NIST CSF is globally recognized and respected, making it a valuable standard for organisations looking to enhance their cybersecurity posture and gain international credibility. By

following the NIST CSF, organisations can improve their risk management processes, identifying and addressing potential vulnerabilities before they can be exploited.

While the NIST CSF itself is not a certification or mandatory requirement, it supports compliance with various regulatory and industry standards, helping organisations meet legal and contractual obligations. The NIST CSF encourages continuous improvement in cybersecurity practices, helping organisations stay ahead of evolving threats and maintain a resilient security posture.

More information about this framework is available at: https://www.nist.gov/cyberframework

3. Self-evaluation questions

Each category of the Expanded Self-Assessment Cybersecurity Framework for SMEs contains 5 questions, across 6 categories, totaling 30 questions across 6 categories.

The six categories are as follows:

1. Firewalls and Internet Gateways
2. Secure Configuration
3. User Access Control
4. Malware Protection
5. Asset Management
6. Backups

Below is the list of topics, questions, and their mapping to the corresponding topics from NCSC Cyber Essentials and NIST CSF 2.0

	Practice	Question	NCSC Cyber Essentials	NIST CSF 2.0
1.	Firewalls and Internet Gateways			
1.1.	Firewalls and Internet Gateways	Do you have boundary firewalls or internet gateways to protect your network?	Secure Configuration	PR.PT-1, PR.AC-3
1.2.	Firewalls and Internet Gateways	Are firewall configurations regularly reviewed and updated?	Secure Configuration	PR.DS-6
1.3.	Firewalls and Internet Gateways	Do you restrict administrative access to firewalls to authorised personnel only?	User Access Control	PR.AC-4

1.4.	Firewalls and Internet Gateways	Do you have logging and monitoring enabled for firewall activities?	Secure Configuration	DE.AE-3, PR.PT-1
1.5.	Firewalls and Internet Gateways	Are there procedures in place to quickly disable or block malicious IP addresses?	Secure Configuration	PR.IP-10, DE.CM-8
2.	Secure Configuration			
2.1.	Secure Configuration	Are default passwords changed and default accounts disabled?	Secure Configuration	PR.AC-1
2.2.	Secure Configuration	Are all software and devices regularly updated?	Patch Management	PR.IP-12
2.3.	Secure Configuration	Is unnecessary software removed from all devices?	Secure Configuration	PR.IP-1, PR.DS-6
2.4.	Secure Configuration	Are auto-run features disabled to prevent unauthorised software execution?	Secure Configuration	PR.IP-1, PR.PT-5
2.5.	Secure Configuration	Is there a process for rolling back updates if necessary?	Patch Management	PR.IP-10
3.	User Access Control			
3.1.	User Access Control	Are user accounts assigned only to authorised individuals?	User Access Control	PR.AC-1
3.2.	User Access Control	Are access levels appropriate to user roles?	User Access Control	PR.AC-4
3.3.	User Access Control	Is multi-factor authentication (MFA) used for sensitive access?	User Access Control	PR.AC-7
3.4.	User Access Control	Are user access rights reviewed and updated regularly?	User Access Control	PR.AC-4
3.5.	User Access Control	Are temporary accounts and access privileges properly managed?	User Access Control	PR.AC-3, PR.AC-5
4.	Malware Protection			

4.1.	Malware Protection	Is anti-malware software installed on all devices?	Malware Protection	PR.IP-12
4.2.	Malware Protection	Are regular scans conducted to detect malware?	Malware Protection	DE.CM-4
4.3.	Malware Protection	Are malware definitions updated automatically?	Malware Protection	PR.IP-12
4.4.	Malware Protection	Is there a procedure for responding to malware detections?	Malware Protection	RS.RP-1, RS.CO-2
4.5.	Malware Protection	Are employees trained to recognize and avoid malware?	Malware Protection	PR.AT-1, PR.AT-2
5.	Asset Management			
5.1.	Asset Management	Do you maintain an up-to-date inventory of all hardware devices on the network?	Asset Management	ID.AM-1
5.2.	Asset Management	Is software inventory maintained and regularly updated to include all installed applications?	Asset Management	ID.AM-2
5.3.	Asset Management	Are assets classified based on their criticality and business value?	Asset Management	ID.BE-3, PR.IP-1
5.4.	Asset Management	Are ownership and responsibility for each asset clearly defined and documented?	Asset Management	ID.AM-6
5.5.	Asset Management	Are asset inventories regularly reviewed and validated against actual assets?	Asset Management	ID.AM-1, ID.AM-2
6.	Backups			
6.1.	Backups	Are regular backups of critical data performed and verified?	Backup Management	PR.IP-4
6.2.	Backups	Are backup copies stored in a secure off-site location?	Backup Management	PR.IP-4
6.3.	Backups	Are backups encrypted to protect data integrity and confidentiality?	Backup Management	PR.DS-1

6.4.	Backups	Is there a defined backup and recovery policy that includes regular testing of the backup system?	Backup Management	PR.IP-4, PR.IP-9
6.5.	Backups	Are backups retained for a sufficient period to ensure data recovery in case of incidents?	Backup Management	PR.IP-4

The detailed research table with specific questions, explanations, and mappings to the NCSC Cyber Essentials and NIST CSF 2.0 frameworks is provided in the Annex 1. This table serves as a comprehensive reference to understand the requirements and improve the SME's cybersecurity practices.

4. Algorithm for Evaluation

Scoring

This framework uses a point-based system to evaluate the cybersecurity posture of SMEs. Each category contains 5 questions, with each question valued at one point, for a total of 30 points across 6 categories. The questions within each category span from basic to advanced, showcasing that the user has implemented progressively more advanced measures and controls. Answering "Yes" to the second question indicates that more advanced measures are in place compared to the first question, increasing cybersecurity and resilience. The same applies when comparing the third question to the second, and so on. The questions within each category span from basic to advanced, showcasing that the user has implemented progressively more advanced measures and controls. Answering "Yes" to the second question indicates that more advanced measures are in place compared to the first question, increasing cybersecurity and resilience. The same applies when comparing the third question to the second, and so on. The evaluation process is as follows:

1. Answer each question with "Yes" or "No/I don't know."
2. For every "Yes" answer, assign one point and move to the next question within the same category.
3. For every "No/I don't know" answer, stop scoring in that category and move to the next category.
4. Each category has a maximum of 5 points.

Level of Preparedness

The score is then used to determine the organisation's level of preparedness:

Level 0: Unsatisfactory Preparedness: Indicates significant gaps in their cybersecurity practices that need to be addressed urgently.

Level 1: Basic Preparedness: Indicates a basic level of cybersecurity, with fundamental practices in place. Organisations at this level should prioritise addressing gaps in their cybersecurity posture.

Level 2: Intermediate Preparedness: Indicates an intermediate level of cybersecurity, with more comprehensive measures in place. Organisations at this level should continue to enhance their cybersecurity practices and address any remaining vulnerabilities.

Level 3: Advanced Preparedness: Indicates an advanced level of cybersecurity, with robust measures in place. Organisations at this level have a strong cybersecurity posture but should maintain vigilance and continue to adapt to new threats.

Determining the Level of Preparedness

The algorithm for determining the organisation's level of preparedness is implemented as follows:

1. Evaluate Level 3: Advanced Preparedness

- Check if the organisation scores at least 4 points in every category.
- If the answer is yes for all categories, the organisation is at Level 3.
- If the answer is no for any category, proceed to the next evaluation level.

2. Evaluate Level 2: Intermediate Preparedness

- Check if the organisation scores at least 3 points in every category.
- If the answer is yes for all categories, the organisation is at Level 2.
- If the answer is no for any category, proceed to the next evaluation level.

3. Evaluate Level 1: Basic Preparedness

- Check if the organisation scores at least 2 points in every category.
- If the answer is yes for all categories, the organisation is at Level 1.
- If the answer is no for any category, conclude and proceed to the recommendations.

4. Evaluate Unsatisfactory

- If the organisation does not meet the criteria for Level 1, they are considered Unsatisfactory. This indicates significant gaps in their cybersecurity practices that need to be addressed urgently.

5. Tailored Recommendations

Once all questions in all categories have been answered, customised recommendations will be provided for each category based on the responses. These recommendations will help organisations identify their specific weaknesses and offer guidance on improving their cybersecurity practices.

The recommendations are structured as follows:

1. Recommendation
2. Implementation Steps
3. Example*

*Disclaimer for the Example: This is just an example and does not constitute a recommendation to use this tool. The mentioned companies and products do not sponsor us, and we are not paid for their mention.

The detailed table with recommendations is provided in the Annex 2.

ANNEX 1 – Questions and Mapping

	Topic	Question	Explanation	NCSC CE	NIST CSF 2.0
1.1	Firewalls and Internet Gateways	Do you have boundary firewalls or internet gateways to protect your network?	Firewalls and internet gateways help protect your network by controlling incoming and outgoing traffic. They act as a barrier between your internal network and external networks, such as the internet. Implementing firewalls is essential for preventing unauthorised access and potential cyber attacks. Regularly updating firewall rules and configurations ensures that your network remains secure against evolving threats.	Boundary Firewalls and Internet Gateways	Function: Protect (PR) Category: Protective Technology (PR.PT) Subcategory: PR.PT-4: Communications and control networks are protected
1.2	Firewalls and Internet Gateways	Are firewall configurations regularly reviewed and updated?	Regularly reviewing and updating firewall configurations ensures that new threats are mitigated and that your network security posture remains robust. Keeping rules and policies up to date is vital for adapting to changing security landscapes.	Secure Configuration	Function: Protect (PR) Category: Protective Technology (PR.PT) Subcategory: PR.PT-1: Removable media is protected and its use restricted according to policy Function: Protect (PR) Category: Maintenance (PR.MA) Subcategory: PR.MA-1: Maintenance and repair of organisational assets are performed and logged in a timely manner, with approved and controlled tools
1.3	Firewalls and Internet Gateways	Do you restrict administrative access to firewalls to authorised personnel only?	Restricting administrative access to firewalls ensures that only qualified and trusted individuals can make changes to critical security settings. This minimises the risk of misconfigurations or unauthorised changes that could weaken network defences.	Access Control	Function: Protect (PR) Category: Identity Management, Authentication, and Access Control (PR.AC) Subcategory: PR.AC-1: Identities and credentials are managed for authorised devices and users Subcategory: PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties

	Topic	Question	Explanation	NCSC CE	NIST CSF 2.0
1.4	Firewalls and Internet Gateways	Do you have logging and monitoring enabled for firewall activities?	Logging and monitoring firewall activities help in detecting and responding to suspicious activities promptly. It allows for a comprehensive audit trail in case of incidents, facilitating quicker forensic analysis and response.	Security Monitoring	Function: Detect (DE) Category: Security Continuous Monitoring (DE.CM) Subcategory: DE.CM-1: The network is monitored to detect potential cybersecurity events Subcategory: DE.CM-7: Monitoring for unauthorised personnel, connections, devices, and software is performed
1.5	Firewalls and Internet Gateways	Are there procedures in place to quickly disable or block malicious IP addresses?	Having procedures to quickly disable or block malicious IP addresses can significantly reduce the window of exposure during an attack. This proactive measure helps in mitigating potential damage from ongoing threats.	Incident Management	Function: Respond (RS) Category: Mitigation (RS.MI) Subcategory: RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks Function: Respond (RS) Category: Communications (RS.CO) Subcategory: RS.CO-2: Incidents are reported consistent with established criteria
2.1	Secure Configuration	Are default passwords changed and default accounts disabled?	Changing default passwords and disabling default accounts prevent unauthorised access through commonly known credentials. This simple step significantly enhances the security of devices and systems.	Secure Configuration	Function: Protect (PR) Category: Identity Management and Access Control (PR.AC) Subcategory: PR.AC-1: Identities and credentials are managed for authorised devices and users

	Topic	Question	Explanation	NCSC CE	NIST CSF 2.0
2.2	Secure Configuration (Security Update Management)	Are all software and devices regularly updated?	Regularly updating software and devices is important because: • Security: Updates often include fixes for security vulnerabilities discovered by developers. Installing these updates reduces the risk of cyberattacks and exploitation of weaknesses. • Performance: Updates can bring improvements in performance and stability of software and devices, resulting in better functionality. • New functionalities: New updates often contain new features and enhancements that can increase productivity and user experience. • Compatibility: Regularly updated software and devices are better compatible with the latest technologies and applications, ensuring smooth operation. • Support: Manufacturers and suppliers usually provide support for the latest versions of software and devices. Regular updates ensure that you receive help and solutions for issues.	Patch Management	Function: Protect (PR) Category: Maintenance (PR.MA) Subcategory: PR.MA-2: Maintenance and repair of organisational assets are performed and logged in a timely manner, with approved and controlled tools Function: Protect (PR) Category: Protective Technology (PR.PT) Subcategory: PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
2.3	Secure Configuration	Is unnecessary software removed from all devices?	Removing unnecessary software reduces the attack surface by eliminating potential vulnerabilities that can be exploited. This practice ensures that only essential applications are present, lowering the risk of exploitation.	Secure Configuration	Function: Protect (PR) Category: Maintenance (PR.MA) Subcategory: PR.MA-2: Remote maintenance of organisational assets is approved, logged, and performed in a manner that prevents unauthorised access

	Topic	Question	Explanation	NCSC CE	NIST CSF 2.0
2.4	Secure Configuration	Are auto-run features disabled to prevent unauthorised software execution?	Disabling auto-run features prevents the automatic execution of potentially malicious software from external media. This control helps protect systems from malware that relies on auto-execution to spread.	Secure Configuration	Function: Protect (PR) Category: Protective Technology (PR.PT) Subcategory: PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations
2.5	Secure Configuration (Security Update Management)	Is there a process for rolling back updates if necessary?	Having a process for rolling back updates allows for quick recovery if an update causes problems. This ensures minimal disruption to operations while maintaining security.	Patch Management	Function: Protect (PR) Category: Maintenance (PR.MA) Subcategory: PR.MA-2: Maintenance and repair of organisational assets are performed and logged in a timely manner, with approved and controlled tools.
3.1	User Access Control	Are user accounts assigned only to authorised individuals?	Assigning user accounts to only authorised individuals limits access to sensitive information and systems. This practice reduces the risk of insider threats and unauthorised access, which can lead to data breaches or system compromises. Implementing access controls and regularly reviewing user permissions helps ensure that only necessary access is granted.	Access Control	Function: Protect (PR) Category: Identity Management and Access Control (PR.AC) Subcategory: PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorised devices, users, and processes.

	Topic	Question	Explanation	NCSC CE	NIST CSF 2.0
3.2	User Access Control	Are access levels appropriate to user roles?	Ensuring that access levels are appropriate to user roles helps in maintaining the principle of least privilege. This minimises the potential damage from compromised accounts by limiting access to only what is necessary for users to perform their duties.	Access Control	Function: Protect (PR) Category: Identity Management and Access Control (PR.AC) Subcategory: PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
3.3	User Access Control	Is multi-factor authentication (MFA used for sensitive access?	Multi-factor authentication provides an additional layer of security by requiring more than one form of verification before granting access. This significantly reduces the risk of unauthorised access from compromised credentials. For instance, when logging into an online banking account, multi-factor authentication might require you to enter your password (something you know) and then input a code sent to your phone (something you have). This way, even if someone steals your password, they still can't access your account without the code from your phone.	Access Control	Function: Protect (PR) Category: Identity Management and Access Control (PR.AC) Subcategory: PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organisational risks).
3.4	User Access Control	Are user access rights reviewed and updated regularly?	Regularly reviewing and updating user access rights ensures that permissions align with current roles and responsibilities. This helps in promptly removing access for users who no longer need it, reducing the risk of excess privileges.	Access Control	Function: Protect (PR) Category: Identity Management and Access Control (PR.AC) Subcategory: PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).

	Topic	Question	Explanation	NCSC CE	NIST CSF 2.0
3.5	User Access Control	Are temporary accounts and access privileges properly managed?	Properly managing temporary accounts and access privileges ensures that they are disabled or removed once they are no longer needed. This prevents orphaned accounts from becoming potential security risks.	Access Control	Function: Protect (PR) Category: Identity Management and Access Control (PR.AC) Subcategory: PR.AC-3: Remote access is managed.
4.1.	Malware Protection	Is anti-malware software installed on all devices?	Anti-malware software detects and prevents malicious software from causing harm to your systems. Regular scans and updates are crucial for maintaining protection against new threats. Ensuring that all devices are equipped with up-to-date anti-malware solutions helps safeguard your organisation from malware infections, including viruses, ransomware, and spyware.	Malware Protection	Function: Protect (PR) Category: Security Continuous Monitoring (DE.CM) Subcategory: DE.CM-8: Vulnerability scans are performed.
4.2	Malware Protection	Are regular scans conducted to detect malware?	Conducting regular scans helps in early detection of malware, allowing for timely intervention and removal. This proactive approach minimizes the impact of malware infections.	Malware Protection	Function: Protect (PR) Category: Security Continuous Monitoring (DE.CM) Subcategory: DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.
4.3	Malware Protection	Are malware definitions updated automatically?	Automatic updates of malware definitions ensure that the anti-malware software can recognize and defend against the latest threats. Keeping definitions current is essential for effective malware protection.	Malware Protection	Function: Protect (PR) Category: Security Continuous Monitoring (DE.CM) Subcategory: DE.CM-1: The network is monitored to detect potential cybersecurity events.

	Topic	Question	Explanation	NCSC CE	NIST CSF 2.0
4.4	Malware Protection	Is there a procedure for responding to malware detections?	Having a defined procedure for responding to malware detections ensures that incidents are handled promptly and effectively. This reduces the potential damage and speeds up recovery.	Incident Management	Function: Respond (RS) Category: Response Planning (RS.RP) Subcategory: RS.RP-1: Response plan is executed during or after an incident.
4.5	Malware Protection	Are employees trained to recognize and avoid malware?	Training employees to recognize and avoid malware helps in preventing infections through user actions. Education and raising awareness of your employees can significantly reduce the likelihood of malware being introduced via phishing or other social engineering tactics. Employees are your biggest allies in fighting for security of your organization. Invest in their knowledge and readiness!	User Education and Awareness	Function: Protect (PR) Category: Awareness and Training (PR.AT) Subcategory: PR.AT-1: All users are informed and trained.
5.1	Asset Management	Do you maintain an up-to-date inventory of all hardware devices on the network?	Keeping an up-to-date inventory of all hardware devices helps ensure that all devices connected to the network are accounted for and can be managed and secured effectively. Good practice is to allow access and usage of your organization networks and resources only to approved devices. This practice helps prevent unauthorised devices from accessing the network and allows for quicker identification and resolution of any security issues related to hardware.	Asset Management	Function: Identify (ID) Category: Asset Management (ID.AM) Subcategory: ID.AM-1: Physical devices and systems within the organisation are inventoried.

	Topic	Question	Explanation	NCSC CE	NIST CSF 2.0
5.2	Asset Management	Is software inventory maintained and regularly updated to include all installed applications?	Maintaining a software inventory that is regularly updated ensures that all software applications used within the organisation are known and managed. This helps in keeping the software up-to-date with the latest security patches and reduces the risk of vulnerabilities due to outdated or unapproved applications.	Asset Management	Function: Identify (ID) Category: Asset Management (ID.AM) Subcategory: ID.AM-2: Software platforms and applications within the organisation are inventoried.
5.3	Asset Management	Are asset inventories regularly reviewed and validated against actual assets?	Regularly reviewing and validating asset inventories against actual assets helps to maintain accurate records of the organisation's resources. This practice helps identify any discrepancies or unauthorised changes, ensuring that all assets are accounted for and properly managed.	Asset Management	Function: Identify (ID) Category: Asset Management (ID.AM) Subcategory: ID.AM-3: Organisational communication and data flows are mapped.
5.4	Asset Management	Are ownership and responsibility for each asset clearly defined and documented?	Clearly defining and documenting ownership and responsibility for each asset ensures that there is accountability for managing and protecting these assets. Knowing who is responsible for each asset helps in ensuring that security measures are properly implemented and maintained.	Asset Management	Function: Identify (ID) Category: Asset Management (ID.AM) Subcategory: ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.

	Topic	Question	Explanation	NCSC CE	NIST CSF 2.0
5.5	Asset Management	Are assets classified based on their criticality and business value?	Classifying assets based on their importance to the organisation's operations and security allows for prioritisation of protection efforts. Critical assets that are essential for business operations can be given higher security measures to ensure they are well protected, minimising the impact of any potential security incidents.	Asset Management	Function: Identify (ID) Category: Asset Management (ID.AM) Subcategory: ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritised based on their classification, criticality, and business value.
6.1	Backups	Are regular backups of critical data performed and verified?	Regularly performing and verifying backups of critical data ensures that there are reliable copies available in case of data loss due to incidents like cyberattacks, hardware failures, or accidental deletion. Verifying the backups ensures that the data can be restored accurately when needed.	Backing up Data	Function: Protect (PR) Category: Data Security (PR.DS) Subcategory: PR.DS-1: Data-at-rest is protected.
6.2	Backups	Are backup copies stored in a secure off-site location?	Storing backup copies in a secure off-site location provides additional protection in case of physical disasters such as fires, floods, or theft at the primary site. This ensures that the data remains safe and can be recovered even if the primary location is compromised.	Backing up Data	Function: Protect (PR) Category: Data Security (PR.DS) Subcategory: PR.DS-5: Protections against data leaks are implemented.

	Topic	Question	Explanation	NCSC CE	NIST CSF 2.0
6.3	Backups	Are backups encrypted to protect data integrity and confidentiality?	Encrypting backups ensures that the data remains confidential and intact, preventing unauthorised access and tampering. This adds an extra layer of security to the backup data, making sure that even if the backup media is lost or stolen, the data cannot be easily accessed or altered.	Backing up Data	Function: Protect (PR) Category: Data Security (PR.DS) Subcategory: PR.DS-2: Data-in-transit is protected.
6.4	Backups	Is there a defined backup and recovery policy that includes regular testing of the backup system?	Having a defined backup and recovery policy that includes regular testing ensures that the backup process is reliable and effective. Regular testing verifies that the backups can be successfully restored, confirming that the organisation can recover from data loss incidents swiftly and effectively.	Backing up Data	Function: Recover (RC) Category: Recovery Planning (RC.RP) Subcategory: RC.RP-1: Recovery plan is executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
6.5	Backups	Are backups retained for a sufficient period to ensure data recovery in case of incidents?	Retaining backups for a sufficient period ensures that the organisation can recover data from an appropriate point in time.This practice helps in restoring data to its state before an incident occurred, minimising data loss and ensuring business continuity, as well as legal compliance.	Backing up Data	Function: Protect (PR) Category: Data Security (PR.DS) Subcategory: PR.DS-3: Data-at-rest is protected to ensure its confidentiality, integrity, and availability.

ANNEX 2 – Tailored recommendations

Disclaimer for the Examples: This is just an example and does not constitute a recommendation to use this tool. The mentioned companies and products do not sponsor us, and we are not paid for their mention.

	Topic	Question	Recommendation	How to Do It	Example:
1.1	Firewalls and Internet Gateways	Do you have boundary firewalls or internet gateways to protect your network?	Install a firewall to act as a barrier between your internal network and external threats. Firewalls control incoming and outgoing network traffic based on predetermined security rules.	If your internet router has a built-in firewall, ensure it is activated. For a more robust solution, consider free firewall software.	**Router Firewall:** Ensure the firewall on your router (e.g., Netgear, TP-Link) is enabled. Most modern routers come with a firewall feature that can be activated through the router's settings page. **Free Firewall Software:** Install pfSense (an open-source firewall solution) or ZoneAlarm (a free firewall for individual users) to add an extra layer of security.
1.2	Firewalls and Internet Gateways	Are firewall configurations regularly reviewed and updated?	Regularly check and update the settings of your firewall to ensure it is functioning correctly and providing the best protection.	Set a reminder to review your firewall settings every month. Look for updates from the firewall software provider and apply them.	**Router Firewall:** Log in to your router's admin page (e.g., 192.168.1.1 for many routers) and review the firewall settings monthly. Check the manufacturer's website for firmware updates. **Firewall Software:** For software like pfSense, log in to the admin interface and check for any notifications about updates or necessary configuration changes.

	Topic	Question	Recommendation	How to Do It	Example:
1.3	Firewalls and Internet Gateways	Do you restrict administrative access to firewalls to authorised personnel only?	Limit access to your firewall's settings to only those who need it, and use strong passwords to protect this access.	Create unique accounts for each administrator with strong passwords. Avoid using default usernames and passwords.	**Router Firewall:** Change the default admin password to a strong password using a mix of letters, numbers, and symbols. Only share this password with trusted personnel. **Firewall Software:** For software like pfSense or ZoneAlarm, create separate admin accounts for each person who needs access, and use strong, unique passwords for each account.
1.4	Firewalls and Internet Gateways	Do you have logging and monitoring enabled for firewall activities?	Enable logging on your firewall to keep a record of all activities and monitor for any unusual behaviour.	Access your firewall's settings and enable the logging feature. Regularly check the logs for any suspicious activity.	**Router Firewall:** Enable the logging feature in your router's settings. Most routers, such as those from Asus or Linksys, have an option to turn on logging. **Firewall Software:** In pfSense, go to the "Status" menu and enable logging for different types of traffic. Check these logs regularly for any anomalies.
1.5	Firewalls and Internet Gateways	Are there procedures in place to quickly disable or block malicious IP addresses?	Create a plan to quickly block any suspicious IP addresses that attempt to access your network.	Familiarise yourself with your firewall's interface so you can quickly block an IP address if needed. Have a list of steps to follow in case of an incident.	**Router Firewall:** Learn how to block IP addresses on your router. For example, on a Netgear router, you can go to the "Advanced" tab, select "Security," and then "Block Sites." **Firewall Software:** In pfSense, navigate to the "Firewall" tab, select "Rules," and add a rule to block the suspicious IP address. Keep a printed copy of these steps for quick reference.

	Topic	Question	Recommendation	How to Do It	Example:
2.1	Secure Configuration	Are default passwords changed and default accounts disabled?	Change all default passwords and disable default accounts to enhance security.	Access the settings of each device and software to change default passwords to strong, unique ones and disable any default accounts.	**Router/Devices:** Log in to your device settings (e.g., Netgear, TP-Link) and change the default admin password. **Software:** Change default passwords and disable default accounts in software settings. Use a password manager like Bitwarden to generate and store strong passwords.
2.2	Secure Configuration (Security Update Management)	Are all software and devices regularly updated?	Ensure all software and devices are regularly updated with the latest security patches.	Enable automatic updates for software and devices whenever possible. Set reminders to check for updates manually if automatic updates are not available.	**Operating Systems:** Enable automatic updates in Windows, macOS, or Linux. **Software:** Use tools like Ninite to keep software up to date. **Devices:** Check for firmware updates on your router or other devices regularly (Netgear Firmware Updates, TP-Link Firmware Updates).
2.3	Secure Configuration	Is unnecessary software removed from all devices?	Remove any unnecessary software to reduce potential vulnerabilities.	Go through each device and uninstall software that is not needed. Use tools to identify and remove bloatware.	**Windows:** Use PC Decrapifier or Bulk Crap Uninstaller to remove unnecessary software. **Mac:** Use AppCleaner to uninstall unnecessary applications.

	Topic	Question	Recommendation	How to Do It	Example:
2.4	Secure Configuration	Are auto-run features disabled to prevent unauthorised software execution?	Disable auto-run features to prevent unauthorised software from executing automatically.	Change settings on your devices to disable auto-run features for external media and network drives.	**Windows:** Disable auto-run by modifying the Group Policy or using the Microsoft Fix It tool. **Linux:** Modify the fstab file to disable auto-mounting. **Mac:** Use System Preferences to disable auto-run features.
2.5	Secure Configuration (Security Update Management)	Is there a process for rolling back updates if necessary?	Establish a process to roll back updates in case they cause issues.	Regularly back up your data and system settings before applying updates. Use built-in system tools to create restore points or backups.	**Windows:** Use System Restore to create restore points before updates. **Mac:** Use Time Machine to back up your system. **Linux:** Use tools like Timeshift to create system snapshots. **Backup Solutions:** Use free backup software like Veeam Agent or Cobian Backup to regularly back up your data.
3.1	User Access Control	Are user accounts assigned only to authorised individuals?	Ensure that only authorised individuals have user accounts to minimise the risk of unauthorised access.	Regularly audit user accounts and remove any that are not needed. Only create accounts for those who require access.	**Windows:** Use the built-in user management tool to manage accounts: Control Panel > User Accounts. **Linux:** Use the userdel command to remove unnecessary user accounts. **Open-Source Tools:** Use LDAP Account Manager to manage user accounts in an LDAP directory.

	Topic	Question	Recommendation	How to Do It	Example:
3.2	User Access Control	Are access levels appropriate to user roles?	Assign access levels based on user roles to enforce the principle of least privilege.	Define roles and assign permissions according to the needs of each role. Regularly review and adjust access levels.	**Windows:** Use Local Group Policy Editor to set permissions based on user roles: Run gpedit.msc. **Linux:** Use chmod and chown commands to set file permissions based on user roles. **Open-Source Tools:** Implement FreeIPA for centralised identity management and role-based access control.
3.3	User Access Control	Is multi-factor authentication (MFA used for sensitive access?	Implement MFA for accessing sensitive systems and data to provide an additional layer of security.	Enable MFA on all accounts that have access to sensitive information or critical systems.	**Google Authenticator:** Use Google Authenticator for MFA on various services. **Authy:** Use Authy as an alternative to Google Authenticator. **Open-Source Tools:** Implement privacyIDEA for an open-source MFA solution.
3.4	User Access Control	Are user access rights reviewed and updated regularly?	Regularly review and update user access rights to ensure they remain appropriate.	Set a schedule to review user access rights at least quarterly. Adjust permissions as needed based on role changes or departures.	**Windows:** Use Active Directory to regularly review and update user access rights. **Linux:** Regularly review /etc/passwd and /etc/group files to check user access. **Open-Source Tools:** Use phpLDAPadmin for managing and reviewing user access rights in LDAP directories.

	Topic	Question	Recommendation	How to Do It	Example:
3.5	User Access Control	Are temporary accounts and access privileges properly managed?	Properly manage temporary accounts and access privileges to ensure they are only active for the necessary period.	Create temporary accounts with expiration dates. Regularly audit and remove temporary accounts that are no longer needed.	**Windows:** Use the `net user` command to create accounts with an expiration date: `net user username /add /expires:MM/DD/YYYY`. **Linux:** Use the `useradd` command with the `-e` option to set an expiration date: `useradd -e YYYY-MM-DD username`. **Open-Source Tools:** Manage temporary access with GLPI, an IT asset management and service desk solution that includes user account management features.
4.1.	Malware Protection	Is anti-malware software installed on all devices?	Ensure anti-malware software is installed on all devices to protect against malicious software.	Install reliable, free anti-malware software on all devices.	**Windows/Mac:** Install Malwarebytes Free. **Linux:** Use ClamAV, an open-source antivirus engine. **Cross-Platform:** Install Sophos Home Free for comprehensive protection.
4.2	Malware Protection	Are regular scans conducted to detect malware?	Schedule regular scans to detect and remove malware.	Set up automatic scans on all devices using the installed anti-malware software.	**Malwarebytes:** Schedule regular scans through the settings menu. **ClamAV:** Use `clamscan -r /home` to scan your home directory. Schedule this with cron jobs. **Sophos Home Free:** Use the dashboard to schedule regular scans.

	Topic	Question	Recommendation	How to Do It	Example:
4.3	Malware Protection	Are malware definitions updated automatically?	Enable automatic updates to ensure malware definitions are current.	Configure the anti-malware software to update definitions automatically.	**Malwarebytes:** Enable automatic updates in the settings. **ClamAV:** Use freshclam to update definitions and set up a cron job for regular updates. **Sophos Home Free:** Ensure automatic updates are enabled in the software settings.
4.4	Malware Protection	Is there a procedure for responding to malware detections?	Establish a clear procedure for responding to malware detections.	Create a response plan that includes steps to isolate, identify, and remove detected malware.	**Malwarebytes:** Follow the software's prompts to quarantine and remove detected malware. **ClamAV:** Use clamscan options to move infected files to a quarantine directory. **Sophos Home Free:** Follow the alerts and recommendations provided by the software.
4.5	Malware Protection	Are employees trained to recognize and avoid malware?	Provide training to employees on how to recognize and avoid malware.	Conduct regular training sessions and provide resources on safe practices.	**Online Training:** Use free resources like Google's Phishing Quiz and Cybrary's Free Cyber Security Training to educate employees.
5.1	Asset Management	Do you maintain an up-to-date inventory of all hardware devices on the network?	Keep a current inventory of all hardware devices connected to your network to manage and secure them effectively.	Use free or open-source tools to create and maintain an inventory list. Update the list regularly when new devices are added or removed.	**Open-Source Tools:** Use GLPI to manage your IT assets, including hardware devices. **Free Software:** Try Spiceworks to scan and inventory your network devices automatically.

	Topic	Question	Recommendation	How to Do It	Example:
5.2	Asset Management	Is software inventory maintained and regularly updated to include all installed applications?	Maintain a detailed inventory of all software applications installed on your devices.	Use tools to track software installations and ensure that the inventory is updated regularly to reflect changes.	**Open-Source Tools:** Use OCS Inventory to track software installations across your network. **Free Software:** Use Belarc Advisor for a comprehensive software inventory on individual devices.
5.3	Asset Management	Are assets classified based on their criticality and business value?	Classify assets based on their importance and value to the organisation to prioritise security efforts.	Create categories for assets (e.g., critical, important, low value) and assign each asset to a category based on its impact on business operations.	**Open-Source Tools:** Utilise GLPI to classify and prioritise assets based on their criticality and business value. **Free Templates:** Use templates from Smartsheet to help classify and manage your assets.
5.4	Asset Management	Are ownership and responsibility for each asset clearly defined and documented?	Assign clear ownership and responsibility for each asset to ensure accountability.	Document the owner and responsible party for each asset in your inventory system. Regularly review and update this information.	**Open-Source Tools:** Use Snipe-IT to document ownership and responsibility for all assets. **Free Software:** Use ManageEngine AssetExplorer to track asset ownership and responsibilities.

	Topic	Question	Recommendation	How to Do It	Example:
5.5	Asset Management	Are asset inventories regularly reviewed and validated against actual assets?	Conduct regular audits to ensure that your asset inventory matches the actual physical assets.	Schedule periodic audits to verify the accuracy of your asset inventory. Use tools to facilitate this process.	**Open-Source Tools:** Use GLPI to schedule and conduct regular audits of your assets. **Free Software:** Use Spiceworks to automate and validate your asset inventory against actual devices.
6.1	Backups	Are regular backups of critical data performed and verified?	Regularly back up critical data and verify that the backups are successful.	Use free or open-source backup tools to schedule and perform regular backups. Periodically test the backups to ensure they are working correctly.	**Open-Source Tools**: Use Duplicati to set up and schedule regular backups. **Free Software:** Try Veeam Agent for Windows or Mac for reliable backup solutions.
6.2	Backups	Are backup copies stored in a secure off-site location?	Store backup copies in a secure off-site location to protect against physical damage or theft.	Use cloud storage solutions or physically transport backups to a different location.	**Open-Source Tools:** Use Duplicati with cloud storage services like Google Drive,, Dropbox, or OneDrive. **Free Software:** Utilise free plans from Backblaze or iDrive for secure cloud backup storage.

	Topic	Question	Recommendation	How to Do It	Example:
6.3	Backups	Are backups encrypted to protect data integrity and confidentiality?	Encrypt backups to ensure data integrity and confidentiality.	Enable encryption features in your backup software to secure your data.	**Open-Source Tools:** Use Duplicati to encrypt backups with strong AES-256 encryption. Free Software: Use Veeam Agent for Windows or Mac, which includes encryption options.
6.4	Backups	Is there a defined backup and recovery policy that includes regular testing of the backup system?	Create a detailed backup and recovery policy that includes regular testing of the backup system.	Document the backup procedures, schedule regular tests, and update the policy as needed.	**Free Templates:** Use free templates from Smartsheet to create your backup and recovery policy. Documentation: Follow guidelines from NIST for developing backup and recovery plans.
6.5	Backups	Are backups retained for a sufficient period to ensure data recovery in case of incidents?	Retain backups for an adequate period to ensure data recovery in case of incidents.	Define a retention policy that meets your organisation's needs and complies with relevant regulations.	O**pen-Source Tools:** Configure retention policies in Duplicati to keep backups for the required duration. **Free Software:** Use Veeam Agent to set retention policies for Windows or Mac backups.