Cybersecurity Efficiency optimization: A combination implementation of both NIST and Essential 8 to optimize resources and time.

Contents

[Common problems with cybersecurity framework implementation: 2](#_Toc145254132)

[NIST 2](#_Toc145254133)

[NIST Framework Core 2](#_Toc145254134)

[NIST Framework Implementation Tiers: 3](#_Toc145254135)

[NIST Framework profiles: 3](#_Toc145254136)

[Coordination of Framework Implementation: 4](#_Toc145254137)

[Essential 8 5](#_Toc145254138)

[Essential 8 Maturity Levels: 5](#_Toc145254139)

[ISO27001 security standard 11](#_Toc145254140)

[Benefits of a joint implementation 12](#_Toc145254141)

[Futureproofing of an organisation using joint implementation 13](#_Toc145254142)

# Common problems with cybersecurity framework implementation:

* Resources used are extensive
* Controls can be complex, comprehensive and difficult to understand
* Cost is a huge factor, needing external accreditation and resources.
* Employees being reluctant to change

# NIST

NIST stands for National Institute of Standards and Technology and in the cybersecurity world, they are most famous for their cybersecurity framework commonly referred to as NIST framework. Frameworks like NIST, all aim to manage potential cybersecurity risks and take appropriate actions and controls in reducing and managing such risks. Deploying NIST as a framework allows the company or organisation to clearly state their ‘cybersecurity posture’.

# NIST Framework Core

4 elements of NIST Framework Core: Functions, Categories, Subcategories, Informative references.

**I**dentify, **P**rotect, **D**etect, **R**espond, **R**ecover – Functions

What do these functions mean? To identify what assets within the company require protecting (Risk Assessment, Governance, Risk Management strategies)

How to protect these assets (Awareness and training, Maintenance, Identity management)

How to detect if these assets are being compromised (Continuous monitoring, detection processes)

What actions is needed as a response of a compromise (Incident response, mitigation)

How to recover after a cybersecurity incident. (Recovery planning, communications)

Subcategories – They work in the sense of footnotes or comments regarding categories. (Data security achieved through encryption)

Informative References: External resources or other standards to aid in implementation of the framework. Most notable ones are ISO27001, COBIT, CIS.

# NIST Framework Implementation Tiers:

Tier 1: Partial

* Risk management is partial and on an ad-hoc basis, prioritization is not well established.
* Limited risk management, irregular implementation of such risk management, limited cybersecurity risk awareness.
* There may not be a clear process for training internal staff about cybersecurity risks and options to mitigate these risks
* The organisation is unaware of cyber supply chain risks and does not collaborate with third parties such as threat intelligence, government.

Tier 2: Risk Informed

* Risk management are managed and approved by management. They may not be established as an organisation-wide policy (informal policies)
* Cybersecurity risk aware, however, there is no well-established method of managing these risks.
* Organisation is aware of their role in the cybersecurity ecosystem, however, they share information based on their discretion. Risk response is inconsistent and usually informal.

Tier 3: Repeatable

* Risk management is formalized and consistent (policy), cybersecurity practices are regularly updated based on business, technologies and threats.
* There are well-defined policies, processes, procedures throughout the organisation in risk management.
* Risk management methods are consistent, cybersecurity is considered in all aspects of the company where applicable.
* External collaboration with other companies and entities.
* Formal risk response including documentation such as written agreements.

Tier 4: Adaptive

* Cybersecurity practices are adapted through a knowledge of previous and current cybersecurity using lessons learned and predictive indicators.
* Organisation continually adapts to change in threats and technology.
* Organisation-wide policies addressing potential cybersecurity risks.
* Cybersecurity risk is treated on the same level as financial risk and other key organisational risks.
* Cybersecurity risk management is well integrated into workplace culture.
* News and information about constant evolving risk and technologies are constantly shared within the organisation as well as other third parties.
* This information is also integrated within the cyber supply chain risk and shared with third parties through both formal and informal methods.

# NIST Framework profiles:

A framework profile is the combination of the framework core and implementation tier to the organisation’s needs and resources. An organisation can have many framework profiles as it combines many of the organisation’s specific needs and requirements to manage cybersecurity risk. These framework profiles also help to build a roadmap in improving an organisation’s cybersecurity risk management and can also help in moving an organisation one tier up in implementation tiers.

# Coordination of Framework Implementation:

NIST framework recommends a cyclic information flow of: Senior Executive making decisions ↔ Business/Process level determining implementation tiers/allocating budget ↔ Operations implementing framework profiles.

NIST also provides in clear steps, how to implement their framework into an organisation and details on what to address in accordance to NIST and improving the organisation’s cybersecurity risk management. Third party requirements are also labelled in detail. There is also advice on self-assessment as well as cybersecurity training of internal staff detailed within NIST framework documentation.

# Essential 8

Essential 8, a cybersecurity framework developed by the Australian Signal Directorate (ASD), to aid in protection against rising cyber threats. It was developed to protect Microsoft Windows-based internet-connected networks. It is called the Essential 8 as it directly addresses the 8 control strategies in order to protect these Microsoft Window based systems. These 8 control strategies are as followed:

1. **Application Control**: Also known as application allowlisting and blocklisting (formerly known as white and blacklist respectively), only allows certain trusted programs to be executed on a system.
2. **Patch Applications**: Regular security patching and updates to OS, software and applications to address known vulnerabilities or in some extreme cases, zero-day vulnerabilities.
3. **Configuration of MS Office macro settings**: Disabling the use of macros or limiting to an extent to only run macros from a trusted source to prevent malicious code execution hidden within documents.
4. **User Application Hardening**: Web browser and other user applications are configured like MS office macros to prevent harmful scripts from being executed.
5. Restricting Administrative privileges: Based off zero trust, users are only assigned their bare minimum privileges and only trusted and authorized personnel are allowed administrative rights.
6. **Patch Operation System**: Similar to patch applications, keeping operating systems up to date to prevent disastrous event such as zero day vulnerabilities.
7. **Multi-factor authentication**: most common forms of MFA are: passwords + SMS, fingerprint + password. MFA prevents malicious users from being able to access systems from just a compromised password alone
8. **Daily backups**: Regular backups of critical data and systems to ensure a swift recovery in the case of a cybersecurity attack or incident.

# Essential 8 Maturity Levels:

Similar to NIST, Essential 8 also has tiers but is named maturity levels ranging from zero to three. Each level starting at the lowest (zero) to highest (3), addresses all 8 control strategies with appropriate and incremental controls. Note that higher tiers include all and if not, improve upon previous tiers. ML 0 has a few technicalities behind it, such as avoiding to implement a particular control strategy while it is deemed feasible to do so, will automatically result in a ML0 regardless of the other controls.

Listed below in tables is, each maturity level’s implementation steps and key differences between each tier.

|  |  |  |  |
| --- | --- | --- | --- |
| Control Strategy | Maturity Level One | Maturity Level Two | Maturity Level Three |
| Application Control | Executables, software libraries, scripts, installers are prevented on workstations by user profiles and temporary folders | Applied on both workstations and internet-facing servers.  Restricting executables, software libraries, scripts, installers etc. to an organisation-approved set.  Allowed and blocked events are all logged. | Applied on all workstations and servers.  Microsoft block recommendations are applied, driver block rules are also implemented.  Application control rulesets are validated yearly or more frequently if needed.  Event logs are secured, protected from unauthorised modification and monitored for compromise.  Response action plan in place in the situation of compromise. |
| Patch Application | Automated asset discovery used fortnightly to detect potential vulnerabilities.  Daily vulnerability scanning with an up to date vulnerability database on internet-facing services.  Fortnightly vulnerability scanning of office workstations and security products.  Patches are applied within two weeks of release, or 48hrs if an exploit is known for internet-facing services, otherwise applied within one month of release.  Workstation services and software not supported by vendors are removed. | Vulnerability are scanned at least fortnightly to identify missing patches.  Patches are applied within two weeks of release.  Patches for other applications are applied within one month. | Patches for workstations are applied within 2 weeks, or 48hrs if an exploit is known.  Applications that are no longer supported are removed. |
| Configuration of Microsoft Office macro settings | Microsoft office macros are switched off and cannot be altered by users without a business requirement for these macros.  Macro antivirus scanning is enabled within Microsoft Office products.  Microsoft Office macros originating from internet are blocked. | Macros are blocked from making WIN32 API calls.  All macro executions within Microsoft Office are logged. | Only macros running within a sandbox environment, digitally signed by a trusted publisher or Trusted Location are allowed to execute.  Only privileged users that validate Microsoft Office macros to be malicious code free are allowed to modify content within Trusted Locations.  All back doors for manually enabling macros (Message Bar, Backstage view) are disabled.  Microsoft Office’s list of trusted publishers is updated annually or more frequently if needed.  Logs are logged centrally and are protected, cannot be modified without authorisation.  Logs are monitored for compromise and there is a plan in place for the event of compromise. |
| User Application Hardening | Web browsers do not process Java or web advertisements from the Internet.  Internet Explorer 11 (IE11) does not process content from the internet.  Web browser security settings cannot be changed by unauthorised users. | ACSC or vendor hardening guidance for web browsers is implemented.  MS Office blocked from creating child processes, executable content, injecting code into other processes.  MS Office configured to prevent activation of OLE packages.  MS Office security settings cannot be changed by users.  PDF software cannot create child processes, ACSC or vendor hardening guidance is implemented for PDF software as well.  PDF software security cannot be configured by users.  PowerShell scripts are blocked and logged. | IE11 is blocked and or removed.  .NET framework 3.5 (2.0 and 3.0 included) is disabled and or removed.  Windows PowerShell 2.0 removed and or disabled.  PowerShell configured to Restrained Language mode.  PowerShell script logs are centrally logged.  Event logs are protected, monitored for compromised and a response plan is in place for the event of compromise. |
| Restrict Administrative Privileges | Requests for privileged access need to be validated upon request.  Privileged accounts cannot access any internet, email and web services.  Privileges users clearly differentiate their privileged and non-privileged operating environments.  Unprivileged accounts cannot login and access privileged accounts. | Privileged accounts only last for 12 months and is automatically disabled unless revalidated.  Privileged access is automatically turned off after 45 days of inactivity.  Privileged operating environments cannot be ran on unprivileged operating environments.  Administrative activities are executed through a jump server.  Credentials for administrator accounts are long, unique, unpredictable and managed, making it difficult to guess.  Privileged access events, group management events are logged. | Privileges access to systems and applications are limited to the tasks and duties of that assigned user (zero trust).  Just-in-time (JIT) administration is used in admin systems and applications.  Windows Defender Credential Guard and Windows Defender Remote Credential Guard are both enabled.  All logs are centrally conducted, monitored and protected. |
| Patch Operating Systems | Automated asset discovery to detect vulnerabilities.  Vulnerability scanning implemented as per Patch Applications section.  Operating systems no longer supported by vendors are replaced. | Weekly vulnerability scanning of operating systems.  Vulnerabilities within operating systems of workstations, servers and network devices are patched within two weeks of release. | Patches are done within 48hrs of a known exploit.  The latest versions of operating systems are used. |
| Multi-Factor Authentication (MFA) | MFA to be used when users authenticating to an organisation’s internet-facing services.  MFA used by organisation’s users for accessing third party services that include storing or communication of organisation’s sensitive data  MFA enabled by default for non-organisational users (with the option to opt out) during authentication to organisation’s internet-facing services. | MFA authentication for privileged users.  MFA authentication uses either an individuals’ possession or knowledge.  Successful and failures of MFA events are logged. | MFA used in important data repositories.  MFA is phishing-resistant in nature.  Event logs are centrally logged, protected and monitored. |
| Regular Backups | Backups of important data, software and configuration settings are performed in accordance to business continuity requirements.  Restoration points are available from backups.  Backups are secured and tested as part of disaster recovery.  Access to backups are not available to unprivileged accounts. | Privileged accounts can only access backups belonging to their own accounts and not any other privileged accounts.  Backups cannot be deleted except for backup administrator accounts. | Unprivileged **and** privileged users cannot access any backup files, including their own.  No account can delete or modify backup during their retention period. |

# ISO27001 security standard

ISO27001:2013 or 2022 edition is a commonly used industry security standard used in Australia and globally. ISO27001 lists the foundation for an organisation to establish, implement, maintain and continually improving an Information Security Management System (ISMS). ISO27001 is very flexible, making it very ideal for many organisations as the standard can be implemented with the organisations’ needs in mind.

ISO27001 lists out the steps to develop an ISMS from scratch for the organisation, following a methodical and logical order.

1. Scope and purpose: defining the boundaries of information security to be managed, addressing the CIA triad (confidentiality, integrity and availability) of information assets.
2. Risk management: Identify and assess information security risks, developing risk treatment plans, developing TVA matrix and other cyber defense matrix.
3. Top Management: defining senior leaders for implementation and support of the ISMS.
4. Context of the organisation: identifying and understanding the internal and external factors that can affect information security (interested parties, legal requirements, business goals.)
5. Information security policy: an official statement outlining the organisation’s information security and its expectations towards compliance.
6. Risk assessment and treatment: building from previous risk management, evaluation of potential risks, threats, and vulnerabilities to current and future potential information assets, development of strategies and prevention methods to protect information assets. These strategies can include, acceptance of certain risks, mitigation, transferring to a third party or avoiding taking such risks.
7. Support within the organisations: implementing of an awareness and training program for all employees can further bolster the strength and effectiveness of an ISMS within an organisation. Documentation and communication guarantee that information security requirements are well understood and acted upon within the organisation.
8. Controls and their objectives: A big portion of ISO27001, there is an additional Annex A section detailing all currently feasible controls and their objectives. These are implemented differently according to an organisation’s needs.
9. Evaluation of ISMS: constant monitoring, analysis, and evaluation of ISMS’s performance within the organisation. Regular internal audits can address compliance and effectiveness issues.
10. Improvement of ISMS: ISO27001 standard places a high importance of regular improvements of ISMS, these improvements can be a results of audit findings, management reviews or a combination of other factors.
11. Implementation of improvements: These improvements can be linked back to Annex A for controls, and they include other types of security such as physical and human resource security which directly impacts the effectiveness of ISMS.
12. Certification and Auditing: Organisations can seek ISO27001 certification through auditing by a certified third party. The organisation will only be certified if it is compliant with ISO27001 standards.

# Benefits of a joint implementation

By combining aspects of NIST framework core and Essential 8’s thorough controls strategies, organisation can save time, resources whilst making sure all aspects of both framework are thoroughly covered such that accreditation and audits later down the line are much easier for external companies and bolstering the organisation’s cybersecurity.

NIST and Essential 8 frameworks both share one key similarity: NIST Implementation Tiers and Maturity levels. Although covered slightly differently, they both cover two key importances in staying relevant in current cybersecurity: Adaptability and Flexibility.

Both NIST and Essential 8 frameworks highlights the importance of staying up to date with modern and evolving cyber threats, which both frameworks directly address in the highest tiers of their framework implementation (Tier 4: Adaptive for NIST and Maturity level three for Essential 8).

Both frameworks are highly adaptable and customisable to the organisation’s needs, they allow for lower levels of implementation if the organisation’s resources do not fit the highest level of implementation needs and provides clear steps in the situation they want to advance their cybersecurity level in either NIST or Essential 8 or both.

Another way that these two frameworks help with implementation while catering for an organisation’s resources is their phased implementation. Phased implementation allows for organisations to prioritise their high risks identified from the early stages of implementation and assign controls accordingly then addressing other lower priority risks. This is also particularly useful in organisations that lack resources or manpower, allowing them to focus their efforts on one crucial area before focusing on the whole framework as a whole.

As both NIST and Essential 8 do not list strict rules in terms of controls and implementation, they are flexible innately. This allows the organisations to implement their controls accordingly to their resources and their needs. This also allows them to integrated with other frameworks and standards such as ISO27001, PCI DSS, COBIT, GDPR to name a few. Integrating these standards if the organisation’s needs and resources allow them can save them even more resources during implementation and accreditation.

A very important point highlighted in both frameworks is communications and documentation. Both frameworks highlight the importance of communication within the organisation as part of their implementation whether it is through employee training or through policies. Both frameworks at their highest levels also require organisations to have a formal policy enforced throughout the organisation to keep their security consistent and complaint. There is also a requirement for new vulnerabilities to be reported formally and acted up on swiftly.

An implementation of both NIST and Essential 8 greatly benefits an organisation that wishes to expand globally as it covers all aspects of cybersecurity to an accredited standard that potential stakeholders can trust. It also allows the organisation to save on both time and resources instead of implementing each framework separately as overlaps in controls are covered thoroughly. Gaps and weaknesses in either framework would be covered as well since a combination of both frameworks ensures that all aspects of cybersecurity and protected and addressed formally through a list of controls and external contacts.

A decrease in resources and time used in implementation also means an increase in Return on Investment (ROI). This increase in ROI means that it will save money and resources for the organisation both initially and eventually as the framework develops and the company expands. NIST also requires a cost benefit-analysis to be conducted and recommends using NIST profiles to aid in this analysis.

# Futureproofing of an organisation using joint implementation

Through a joint implementation, an organisation can be future proofed through the building of an incident response plan as required by higher levels of Essential 8. This incident response plan can also be communicated and shared between external vendors to prepare for the event of a cybersecurity event.

This also paves the way for the continuous information flow between vendors and organisations which is required by NIST at the Tier 3 or Tier 4 and can help organisations at those lower tiers, to implement higher in NIST standards. This in combination, with documentation, can allow organisations to reach out to new and more specific external vendors as they grow their framework security level, and allow for potential business partners to trust in their cybersecurity structure.

Utilising NIST framework profiles and cost-benefit analysis, it is possible to determine whether higher implementation levels of either or both NIST and Essential 8 is feasible for the organisation given their resources. This allows the frameworks to be both flexible as the organisation grows and expands their network and information.

It is also possible for these frameworks to accompany other well-accredited security standards such as COBIT, ISO27001 and PCI DSS to name a few. The frameworks strongly suggest including standards within the implementation as the organisation sees fit and they can share that they are accredited with such standards for stakeholders to trust that their information and cybersecurity is up to industry standards