tripwire
by HelpSystems

Tripwire Product Mapping to the NIS Directive – CAF v2.0

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

NIS Directive - CAF Version 2.0 Mapping

Statements in blue indicate where Tripwire product(s) meet the objective.

CAF - Objective A - Managing security risk

A1 Governance

Principle

The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems.

A1.a Board direction

You have effective organisational security management led at board level and articulated clearly in corresponding policies.

Not Achieved	Achieved
At least one of the following statements is true	All the following statements are true
The security of network and information systems related to the delivery of essential services is not discussed or reported on regularly at board-level.	Your organisation's approach and policy relating to the security of networks and information systems supporting the delivery of essential services are set and managed at board level. These are communicated, in a meaningful way, to risk management decision-makers across the organisation.
Board-level discussions on the security of networks and information systems are based on partial or out-of-date information, without the benefit of expert guidance.	Regular board discussions on the security of network and information systems supporting the delivery of your essential service take place, based on timely and accurate information and informed by expert guidance.
The security of networks and information systems supporting your essential services is not driven effectively by the direction set at board level.	There is a board-level individual who has overall accountability for the security of networks and information systems and drives regular discussion at board-level.
Senior management or other pockets of the organisation consider themselves exempt from some policies, or expect special accommodations to be made.	Direction set at board level is translated into effective organisational practices that direct and control the security of the networks and information systems supporting your essential service.

A1.b Roles and responsibilities

Your organisation has established roles and responsibilities for the security of networks and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.

Not Achieved	Achieved
At least one of the following statements is true	All the following statements are true
Key roles are missing, left vacant, or fulfilled on an ad-hoc or informal basis.	Necessary roles and responsibilities for the security of networks and information systems supporting your essential service have been identified. These are reviewed periodically to ensure they remain fit for purpose.
Staff are assigned security responsibilities but without adequate authority or resources to fulfil them.	Appropriately capable and knowledgeable staff fill those roles and are given the time, authority, and resources to carry out their duties.
Staff are unsure what their responsibilities are for the security of the essential service.	There is clarity on who in your organisation has overall accountability for the security of the networks and information systems supporting your essential service.

A1.c Decision-making

You have senior-level accountability for the security of networks and information systems, and delegate decision-making authority appropriately and effectively. Risks to network and information systems related to the delivery of essential services are considered in the context of other organisational risks.

Not Achieved	Achieved
At least one of the following statements is true	All the following statements are true
What should be relatively straightforward risk decisions are constantly referred up the chain, or not made.	Senior management have visibility of key risk decisions made throughout the organisation.
Risks are resolved informally (or ignored) at a local level without a formal reporting mechanism when it is not appropriate.	Risk management decision-makers understand their responsibilities for making effective and timely decisions in the context of the risk appetite regarding the essential service, as set by senior management.
Decision-makers are unsure of what senior management's risk appetite is, or only understand it in vague terms such as "averse" or "cautious".	Risk management decision-making is delegated and escalated where necessary, across the organisation, to people who have the skills, knowledge, tools, and authority they need.
Organisational stovepipes result in risk decisions being made in isolation, for example, engineering and IT don't talk to each other about risk.	Risk management decisions are periodically reviewed to ensure their continued relevance and validity.
Risk priorities are too vague to make meaningful distinctions between them, for example almost all risks are rated 'medium' or 'amber'.	

A2 Risk Management	
Principle	
The organisation takes appropriate steps to identify, assess and understand security risks to the network and information systems supporting the delivery of essential services. This includes an overall organisational approach to	

A2.a Risk Management Process	
Your organisation has effective internal processes for managing risks to the security of network and information systems related to the delivery of essential services, and communicating associated activities.	
Not Achieved	**Achieved**
At least one of the following statements is true	All the following statements are true
Risk assessments are not based on a clearly defined set of threat assumptions.	Your organisational process ensures that security risks to networks and information systems relevant to essential services are identified, analysed, prioritised, and managed.
Risk assessment outputs are too complex or unwieldy to be consumed by decision-makers, and are not effectively communicated in a clear and timely manner.	Your approach to risk is focused on the possibility of disruption to your essential service, leading to a detailed understanding how such disruption might arise as a consequence of possible attacker actions and the security properties of your networks and information systems.
Risk assessments for critical systems are a "one- off" activity (or not done at all).	Your risk assessments are based on a clearly articulated set of threat assumptions, informed by an up-to-date understanding of security threats to your essential service.
The security element of project or programme milestones are solely dependent on completing the risk management process.	Your risk assessments are informed by an understanding of the vulnerabilities in the networks and information systems supporting your essential service.
One single approach to assessing risks is applied to every risk management problem within the organisation.	The output from your risk management process is a clear set of security requirements that will address the risks in line with your organisational approach to security
Systems are assessed in isolation, without consideration of dependencies and interactions with other systems (including interactions between IT and OT environments).	Significant conclusions reached in the course of your risk management process are communicated to key security decision-makers and accountable individuals.
Security requirements and mitigations are arbitrary or are applied from a control catalogue without consideration of how they contribute to the security of the essential service.	You conduct risk assessments when significant events potentially affect the essential service, such as replacing a system or a change in the cyber security threat
Risks remain unresolved on a register for prolonged periods of time awaiting senior decision-making or resource allocation to resolve.	Your risk assessments are dynamic, and are updated in the light of relevant changes which may include technical changes to networks and information systems, change of use and new threat information.
	The effectiveness of your risk management process is reviewed periodically and improvements made as required.

A2.b Assurance	
You have demonstrable confidence in the effectiveness of the security of your technology, people, and processes relevant to essential services.	
Not Achieved	**Achieved**
At least one of the following statements is true	All the following statements are true
A particular product or service is seen as a "silver bullet" and vendor claims are taken at face value.	You validate that the security measures in place to protect the networks and information systems are effective, and remain effective for the lifetime over which they are needed.
Assurance methods are applied without appreciation of their strengths and limitations, such as the risks of penetration testing in operational environments.	You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of essential services.
Assurance is assumed because there have been no known problems to date.	Your confidence in the security as it relates to your technology, people, and processes can be demonstrated to, and verified by, a third party.
	Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.
	The methods used for assurance are reviewed to ensure they are working as intended and remain the most appropriate method to use.

A3 Asset Management	
Principle	
Everything required to deliver, maintain or support networks and information systems for essential services is determined and understood. This includes data, people and systems, as well as any	

A3.a Asset management	
Not Achieved	**Achieved**
At least one of the following statements is true	All the following statements are true
Inventories of assets relevant to the essential service are incomplete, non-existent, or inadequately detailed.	All assets relevant to the secure operation of essential services are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date.
Only certain domains or types of asset are documented and understood. Dependencies between assets are not understood (such as the dependencies between IT and OT).	Dependencies on supporting infrastructure (e.g. power, cooling etc.) are recognised and recorded.

Information assets, which could include personally identifiable information or other sensitive information, are stored for long periods of time with no clear business need or retention policy.	You have prioritised your assets according to their importance to the delivery of the essential service.
Knowledge critical to the management, operation, or recovery of essential services is held by one or two key individuals with no succession plan.	You have assigned responsibility for managing the physical assets.
Asset inventories are neglected and out of date.	Assets relevant to essential services are managed with cyber security in mind throughout their lifecycle, from creation through to eventual decommissioning or disposal.

A4 Supply Chain

Principle

The organisation understands and manages security risks to networks and information systems supporting the delivery of essential services that arise as a result of dependencies on external

A4.a Managing security risks

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
You do not know what data belonging to you is held by suppliers, or how it is managed.	You understand the general risks suppliers may pose to your essential services.	You have a deeper understanding of your supply chain, including sub-contractors and the wider risks it faces. You take into account factors such as supplier's partnerships, competitors, nationality and other organisations with which they sub-contract. This informs your risk assessment and procurement processes.
Elements of the supply chain for essential services are subcontracted and you have little or no visibility of the sub-contractors.	You know the extent of your supply chain for essential services, including sub- contractors.	Your approach to supply chain risk management includes the risks to your essential services arising from supply chain subversion by capable and well- resourced attackers, if this is part of your threat model.
Relevant contracts do not have security requirements.	You engage with suppliers about security, and you set and communicate security requirements in contracts.	You have confidence that information shared with suppliers that might be essential to the service is well protected.
Suppliers have unrestricted or unmonitored access to critical systems, or access that bypasses your own security controls.	You are aware of all third-party connections and have assurance that they meet your organisation's security requirements.	You can clearly express the security needs you place on suppliers in ways that are mutually understood, and are laid in contracts. There is a clear and documented shared-responsibility model.
	Your approach to security incident management considers incidents that might arise in your supply chain.	All network connectivity and data object exchange is appropriately managed.
		Where appropriate, you offer support to suppliers to resolve incidents.

CAF - Objective B - Protecting against cyber-attack

B1 Service Protection Policies and Processes

Principle

The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support delivery of essential services.

B1.a Policy and process development

You have developed and continue to improve a set of service protection policies and processes that manage and mitigate the risk of cyber security-related disruption to the essential service.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All of the following statements are true	All the following statements are true
Your service protection policies and processes are absent or incomplete.	Your service protection policies and processes document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance. Cyber security is often treated as a separate issue.	You document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance. Cyber security is embedded throughout these policies and processes and key performance indicators are reported to your executive management.
Service protection policies and processes are not applied universally or consistently.	You review and update service protection policies and processes in response to major cyber security incidents	Your organisation's service protection policies and processes are developed to be practical, usable and appropriate for your essential service and your technologies.
People often or routinely circumvent service protection policies and processes to achieve business objectives.		Where your service protection policies and processes place requirements on people, e.g. changes in behaviour or activity, this is practical and they can do what is expected.
Your organisation's security governance and risk management approach has no bearing on your service protection policies and processes.		You review and improve policies and processes at suitably regular intervals to ensure they remain relevant to threats, the way people and systems work, adapt to lessons learned and remain appropriate and effective. This is in addition to reviews following a major cyber security incident.
System security depends upon users' careful and consistent application of manual security processes.		Your systems are designed with 'guard rails', so that they remain secure even when user security policies and processes are not always followed.
Service protection policies and processes have not been reviewed in response to major changes (e.g. technology or regulatory framework), or within a suitable period.		
Service protection policies and processes are not readily available to staff, too detailed to remember, or too hard to understand.		

B1.b Policy and process implementation You have successfully implemented your security policies and processes and can demonstrate the security benefits achieved.		
Not Achieved	**Partially Achieved**	**Achieved**
Any of the following statements are true	**All of the following statements are true**	**All the following statements are true**
None or only part of your service protection policies and processes are enacted.	All your service protection policies and processes are enacted and you assess their correct application.	All your service protection policies and processes are enacted. You regularly evaluate the correct application and security effectiveness of your service protection policies.
You do not have an understanding of the impact of your service protection policies and processes on your security.	Your service protection policies and processes are integrated with other organisational policies and processes, including HR assessments of individuals' trustworthiness.	Your service protection policies and processes are integrated with other organisational policies and processes, including HR assessments of individuals' trustworthiness.
Some or all staff are unaware of their responsibilities under your service protection policies and processes.	All staff are aware of their responsibilities under your service protection policies and processes.	Your service protection policies and processes are effectively and appropriately communicated across all levels of the organisation. All staff are aware of their responsibilities under your service protection policies and processes.
You do not detect breaches of service protection policies and processes.	All significant breaches of service protection policies and processes are investigated; less significant breaches are tracked and assessed for trends or aggregation as a larger breach.	Suitable action is taken to correct significant single or aggregated breaches of service protection policies and processes.

B2 Identity and Access Control

Principle

The organisation understands, documents and manages access to systems and functions supporting the delivery of essential services. Users (or automated functions) that can access data or services are appropriately verified, authenticated and authorised.

B2.a Identity verification, authentication and authorisation You robustly verify, strongly authenticate and authorise access to the networks and information systems supporting your essential service.		
Not Achieved	**Partially Achieved**	**Achieved**
Any of the following statements are true	**All of the following statements are true**	**All the following statements are true**
You cannot individually identify all users (whether by user identifier or secondary means) with access to networks or information systems on which your essential service depends.	You individually identify all the users that are granted access to your networks or information systems (both logically and physically), whether by user identifier or alternative / secondary means.	Only individually authenticated and authorised users can connect to or access your networks or information systems. Both logical and physical access require this individual authentication and authorisation.
Unknown or unauthorised users or devices can connect to your networks or information systems.	User access to essential service networks and information systems is limited to the minimum necessary.	User access to all your networks and information systems supporting the essential service is limited to the minimum necessary.
User access is not limited to the minimum necessary.	You use additional authentication mechanisms, such as two-factor or hardware-backed certificates, for access to sensitive systems such as operational technology.	You use additional authentication mechanisms, such as two-factor or hardware- backed certificates, for all systems that operate or support your essential service.
	You individually authenticate and authorise all remote access to all your networks and information systems that support your essential service.	You use additional authentication mechanisms, such as two-factor or hardware- backed certificates, when you individually authenticate and authorise all remote access to all your networks and information systems that support your essential service.
	The list of users with access to essential service networks and systems is reviewed on a regular basis, e.g. annually.	The list of individuals with access to all your networks and systems supporting the essential service is reviewed on a regular basis, e.g. annually.
		The list of users with access to essential service networks and systems is reviewed on a regular basis, e.g. every 6 months.

B2.b Device management You fully know and have trust in the devices that are used to access your networks, information systems and data that support your essential service.		
Not Achieved	**Partially Achieved**	**Achieved**
Any of the following statements are true	**All of the following statements are true**	**All the following statements are true**
Users are allowed to connect to your essential service's networks using personal devices.	Only enterprise-owned and managed devices are allowed to access your essential service's networks and information systems.	Dedicated devices are used for privileged actions (such as administration or accessing the essential service's network and information systems). These devices are not used for directly browsing the web or accessing email.
Administrators are able to perform administrative functions from non-corporately managed devices (such as remote access from personal devices).	All administrative access occurs from dedicated management devices.	You have obtained independent or professional assurance of the security of third-party networks, or you only allow third-party devices / networks dedicated to supporting your systems to connect.
You have not gained assurance in the security of any third-party devices or networks connected to your systems.	You have sought to understand the security properties of third- party devices and networks before they are allowed to be connected to your systems. You have taken appropriate steps to mitigate any risks identified.	You perform device identity management which is cryptographically backed, and only allow known devices to access systems.
Physically connecting to your network gives a device access to systems without further authentication.	The act of connecting to a network port or cable does not grant access to any systems.	You perform regular scans to detect unknown devices and investigate any findings.
	You are able to detect unknown devices being connected to your network, and investigate such incidents.	

B2.c Privileged user management

You closely manage privileged user access to networks and information systems supporting the essential service.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All of the following statements are true	All the following statements are true
You do not know the names of all individuals with privileged access to administer your system (infrastructure, platforms, software, configuration, etc.)	Privileged access requires additional validation, but this does not use a strong form of authentication (e.g. two-factor/ hardware authentication or active monitoring).	Privileged access (e.g. to systems controlling the essential service or system administration) is carried out with separate accounts that are closely managed.
It is not known whether all privileged users are strongly authenticated when accessing the system.	You know the names of all individuals in your organisation and your supply chain with privileged access to your networks and platforms, software, configuration, etc.) information systems (infrastructure,	Where you don't already issue temporary, time-bound rights for privileged access and external third- party support access, you are migrating to access control that supports this functionality.
Privileged access is granted from remote sessions without additional validation.	Activity by privileged users is periodically validated, e.g. annually.	You regularly review privileged access rights and always update privileges as part of your joiners, movers and leavers process.
The list of system administrators has not been reviewed recently, e.g. within the last 12 months.	Privileged users are only granted specific privileged permissions and roles which are essential to their business function.	All privileged access to your networks and information systems requires strong authentication, such as two-factor/ hardware authentication, or additional real- time security monitoring.
Privileged user access is granted on a system-wide basis (as opposed to by specific roles).		Privileged access is only granted on devices owned and managed by your organisation.
System administrators use generic (shared or default name) accounts to administer servers and devices.		Activity by privileged users is routinely validated.
Where there are "always on" terminals which can perform privileged actions (such as in a control room), there are no additional controls (e.g. physical controls) to ensure access is appropriately restricted.		The list of system administrators is regularly reviewed, e.g. every six months.
User roles are not suitably logically segregated, e.g. users have a single user identifier for routine business activities and privileged or segregated roles.		You record and store all privileged user sessions for offline analysis and investigation.

B2.d IDAC management and maintenance

You assure good management and maintenance of identity and access control (IDAC) for your networks and information systems supporting the essential service.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All of the following statements are true	All the following statements are true
Greater rights are granted to users than necessary.	You have a robust procedure to verify each user and issue minimum required access rights.	You have an auditable, robust procedure to verify each user and issue minimum required access rights.
User rights are granted without validation of their identity and requirement for access.	You regularly review access rights and those no longer needed are revoked.	Your joiners, leavers and movers process ensures that, in addition to when people change roles, user permissions are reviewed regularly.
User rights are not reviewed when they move jobs.	Your joiners, leavers and movers process ensures that user permissions are reviewed both when people change roles and at regular intervals.	All access is logged and monitored.
User rights remain active when people leave your organisation.	All access is logged and monitored.	You regularly review access logs and correlate this data with other access records and expected activity.
		Attempts by unauthorised users to connect to your systems are alerted, promptly assessed and investigated where relevant.

B3 Data Security

Principle

Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause disruption to essential services. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for

B3.a Understanding data

You have a good understanding of data important to the delivery of the essential service, where it is stored, where it travels and how unavailability or unauthorised access, modification or deletion would impact the service. This also applies to third parties storing, or accessing data important to the delivery of essential services.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All of the following statements are true	All the following statements are true
You have limited or incomplete knowledge of what data is used by and produced in the delivery of the essential service. You cannot identify the important data on which your essential service relies.	You have identified and catalogued all the data important to the delivery of the essential service, or that would assist an attacker. You know who has access to that data.	You have identified and catalogued all the data important to the delivery of the essential service, or that would assist an attacker. You know who has access to this important data.
You cannot identify who has access to data important to the delivery of the essential service.	You periodically review location, transmission, quantity and quality of data important to the delivery of the essential service.	You maintain a current understanding of the location, quantity and quality of data important to the delivery of the essential service.
You are not able to clearly articulate the impact of data compromise or inaccessibility.	You have identified all mobile devices and media that hold data important to the delivery of the essential service.	You take steps to remove or minimise unnecessary copies or unneeded historic data.
	You understand the impact on your essential service of all relevant scenarios, including unauthorised access, modification or deletion, or when authorised users are unable to appropriately access this data.	You have identified all mobile devices and media that may hold data important to the delivery of the essential service.
	You validate these impact statements regularly, e.g. every 12 or 24 months.	You maintain a current understanding of the data links used to transmit data that is important to your essential service.
		You understand the context, limitations and dependencies of your important data.

		You understand the impact on your essential service of all relevant scenarios, including unauthorised data access, modification or deletion, or when authorised users are unable to appropriately access this data.
		You validate these impact statements regularly, e.g. annually.

B3.b Data in transit

You have protected the transit of data important to the delivery of the essential service. This includes the transfer of data to third parties.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All of the following statements are true	All the following statements are true
You do not know what all your data links are, or which carry data important to the delivery of the essential service.	You have identified and suitably protected all the data links that carry data important to the delivery of the essential service.	You have identified and suitably protected all the data links that carry data important to the delivery of the essential service.
Data important to the delivery of the essential service travels without technical protection over untrusted or openly accessible carriers.	You apply appropriate technical means (e.g. cryptography) to protect data that travels over an untrusted carrier, but you have limited or no confidence in the robustness of the protection applied.	You apply appropriate physical or technical means to protect data that travels over an untrusted carrier, with justified confidence in the robustness of the protection applied.
Critical data paths that could fail, be jammed, be overloaded, etc. have no alternative path.		Suitable alternative transmission paths are available where there is a risk of impact on the delivery of the essential service due to resource limitation (e.g. transmission equipment or service failure, or important data being blocked or jammed).

B3.c Stored data

You have protected stored data important to the delivery of the essential service.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All of the following statements are true	All the following statements are true
You have no, or limited, knowledge of where data important to the delivery of the essential service is stored.	All copies of data important to the delivery of your essential service are necessary. Where this important data is transferred to less secure systems, the data is provided with limited detail and/or as a read-only copy.	You have only necessary copies of this data. Where data is transferred to less secure systems, the data is provided with limited detail and/or as a read-only copy.
You have not protected vulnerable stored data important to the delivery of the essential service in a suitable way.	You have applied suitable physical or technical means to protect this important stored data from unauthorised access, modification or deletion.	You have applied suitable physical or technical means to protect this important stored data from unauthorised access, modification or deletion.
Backups are incomplete, untested, not adequately secured or could be inaccessible in a disaster recovery or business continuity situation.	If cryptographic protections are used, you apply suitable technical and procedural means, but you have limited or no confidence in the robustness of the protection applied.	If cryptographic protections are used you apply suitable technical and procedural means, and you have justified confidence in the robustness of the protection applied.
	You have suitable, secured backups of data to allow the essential service to continue should the original data not be available. This may include off- line or segregated backups, or appropriate alternative forms such as paper copies.	You have suitable, secured backups of data to allow the essential service to continue should the original data not be available. This may include off-line or segregated backups, or appropriate alternative forms such as paper copies.
		Necessary historic or archive data is suitably secured in storage.

B3.d Mobile data

You have protected data important to the delivery of the essential service on mobile devices.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All of the following statements are true	All the following statements are true
You don't know which mobile devices may hold data important to the delivery of the essential service.	You know which mobile devices hold data important to the delivery of the essential service.	Mobile devices that hold data that is important to the delivery of the essential service are catalogued, are under your organisation's control and configured according to best practice for the platform, with appropriate technical and procedural policies in place.
You allow data important to the delivery of the essential service to be stored on devices not managed by your organisation, or to at least equivalent standard.	Data important to the delivery of the essential service is only stored on mobile devices with at least equivalent security standard to your organisation.	Your organisation can remotely wipe all mobile devices holding data important to the delivery of essential service.
Data on mobile devices is not technically secured, or only some is secured.	Data on mobile devices is technically secured.	You have minimised this data on these mobile devices. Some data may be automatically deleted off mobile devices after a certain period.

B3.e Media / equipment sanitisation

You appropriately sanitise data from the service, media or equipment.

Not Achieved	Achieved
Any of the following statements are true	All the following statements are true
Some or all devices, equipment or removable media that hold data important to the delivery of the essential service are disposed of without sanitisation of that data.	You catalogue and track all devices that contain data important to the delivery of the essential service (whether a specific storage device or one with integral storage).
Providers of any cloud services you use are not able to explain how storage is sanitised when it is released.	All data important to the delivery of the essential service is sanitised from all devices, equipment or removable media before disposal.
	Your cloud service providers appropriately sanitise data storage areas before reallocating to another user.

B4 System Security

Principle

Network and information systems and technology critical for the delivery of essential services are protected from cyber-attack. An organisational understanding of risk to essential services informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.

B4.a Secure by design

You design security into the network and information systems that supports the delivery of essential services. You minimise their attack surface and ensure that the delivery of the essential service should not be impacted by the exploitation of any single vulnerability.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All of the following statements are true	All the following statements are true
Systems essential to the operation of the essential service are not appropriately segregated from other systems.	You employ appropriate expertise to design network and information systems.	You employ appropriate expertise to design network and information systems.
Internet access is available from operational systems.	You design strong boundary defences where your networks and information systems interface with other organisations or the world at large.	Your networks and information systems are segregated into appropriate security zones, e.g. operational systems for the essential service are segregated in a highly trusted, more secure zone.
Data flows between the essential service's operational systems and other systems are complex, making it hard to discriminate between legitimate and illegitimate/malicious traffic.	You design simple data flows between your networks and information systems and any external interface to enable effective monitoring.	The networks and information systems supporting your essential service are designed to have simple data flows between components to support effective security monitoring.
Remote or third party accesses circumvent some network controls to gain more direct access to operational systems of the essential service.	You design to make network and information system recovery simple.	The networks and information systems supporting your essential service are designed to be easy to recover.
	All inputs to operational systems are checked and validated at the network boundary where possible, or additional monitoring is in place for content-based attacks.	All inputs to operational systems are transformed and inspected at the border where possible. Where this is not currently possible, content- based attacks are mitigated by other means.

B4.b Secure configuration

You securely configure the network and information systems that support the delivery of essential services.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All of the following statements are true	All the following statements are true
You haven't identified the assets that need to be carefully configured to maintain the security of the essential service.	You have identified and documented the assets that need to be carefully configured to maintain the security of the essential service.	You have identified, documented and actively manage the assets that need to be carefully configured to maintain the security of the essential service.
Your network and information systems have inconsistent security in operating system builds or configurations.	Secure platform and device builds are used across the estate.	All platforms conform to your secure, consistent baseline build, or latest known good configuration version for that environment.
Configuration details are not recorded or lack enough information to be able to rebuild the system or device.	Consistent, secure and minimal system and device configurations are applied across the same types of environment.	You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.
You don't record changes or adjustments to security configuration at security boundaries with the networks and information systems supporting your essential service.	Changes and adjustments to security configuration at security boundaries with the networks and information systems supporting your essential service are approved and documented.	You regularly review and validate that your network and information systems have the expected, secured settings and configuration.
	You verify software before installation is permitted.	Only permitted software can be installed and standard users cannot change settings that would impact security or business operation.
		If automated decision-making technologies are in use, their operation is well understood and decisions can be replicated.

B4.c Secure management

You manage your organisation's network and information systems that support the delivery of essential services to enable and maintain security.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All of the following statements are true	All the following statements are true
Essential service networks and systems are administered or maintained using non-dedicated devices.	Your systems and devices supporting the delivery of the essential service are only administered or maintained by authorised privileged users from dedicated devices.	Your systems and devices supporting the delivery of the essential service are only administered or maintained by authorised privileged users from dedicated devices that are technically segregated and secured to the same level as the networks and systems being maintained.
You do not have good or current technical documentation of your networks and information systems.	Technical knowledge about networks and information systems, such as documentation and network diagrams, is regularly reviewed and updated.	You regularly review and update technical knowledge about networks and information systems, such as documentation and network diagrams, and ensure they are securely stored.
	You prevent, detect and remove malware or unauthorised software. You use technical, procedural and physical measures as necessary.	You prevent, detect and remove malware or unauthorised software. You use technical, procedural and physical measures as necessary.

B4.d. Vulnerability management

You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All of the following statements are true	All the following statements are true
You do not understand the exposure of your essential service to publicly-known vulnerabilities.	You maintain a current understanding of the exposure of your essential service to publicly-known vulnerabilities.	You maintain a current understanding of the exposure of your essential service to publicly-known vulnerabilities.

You do not mitigate externally- exposed vulnerabilities promptly.	Announced vulnerabilities for all software packages, network equipment and operating systems used to support your essential service are tracked, prioritised and externally- exposed vulnerabilities are mitigated (e.g. by patching) promptly.	Announced vulnerabilities for all software packages, network equipment and operating systems used to support your essential service are tracked, prioritised and mitigated (e.g. by patching) promptly.
There are no means to check data or software imports for malware.	Some vulnerabilities that are not externally exposed have temporary mitigations for an extended period.	You regularly test to fully understand the vulnerabilities of the networks and information systems that support your essential service and verify this understanding with third-party testing.
You have not recently tested to verify your understanding of the vulnerabilities of the networks and information systems that support your essential service.	You have temporary mitigations for unsupported systems and software while pursuing migration to supported technology.	You maximise the use of supported software, firmware and hardware in your networks and information systems supporting your essential service.
You have not suitably mitigated systems or software that is no longer supported. These systems may still be running, but not in operational use.	You regularly test to fully understand the vulnerabilities of the networks and information systems that support your essential service.	
You are not pursuing replacement for unsupported systems or software.		

B5 Resilient Networks and Systems

Principle

The organisation builds resilience against cyber-attack and system failure into the design, implementation, operation and management of systems that support the delivery of essential services.

B5.a Resilience preparation

You are prepared for restoring the essential service following disruption.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All of the following statements are true	All the following statements are true
You have limited understanding of all the elements that are required to deliver the essential service.	You know all networks, information systems and underlying technologies that are necessary to deliver the essential service and understand their interdependencies.	You have business continuity and disaster recovery plans that have been tested for practicality, effectiveness and completeness. Appropriate use is made of different test methods, e.g. manual failover, table-top exercises, or red- teaming.
You have not completed business continuity and/or disaster recovery plans for your essential service's networks, information systems and their dependencies.	You know the order in which systems need to be restored to most quickly and effectively restore the essential service.	You use your security awareness, e.g. threat intelligence sources, to make temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware.
You have not fully assessed the practical implementation of these plans.		

B5.b Design for resilience

You design the network and information systems supporting your essential service to be resilient to cyber security incidents. Systems are appropriately segregated and resource limitations are mitigated.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All of the following statements are true	All the following statements are true
Operational networks and systems are not sufficiently segregated.	Operational systems for your essential service are logically separated from your business systems, e.g. they reside on the same network as the rest of the organisation, but within a DMZ. Internet access is not available from operational systems.	You have identified and mitigated all resource limitations, i.e. bandwidth limitations.
Internet services, such as browsing and email, are accessible from essential service operational systems.	Resource limitations (e.g. network bandwidth, single network paths) have been identified but not fully mitigated.	You have identified and mitigated any geographical constraints or weaknesses. For example, systems that your essential service depends upon are duplicated to another location, important network connectivity has alternative physical paths and service providers.
You do not understand or lack plans to mitigate all resource limitations that could adversely affect your essential service.		You review and update dependencies, resource and geographical limitation assessments and update mitigations when required.

B5.c Backups

You hold accessible and secured current backups of data and information needed to recover.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All of the following statements are true	All the following statements are true
Backup coverage is incomplete in coverage and would be inadequate to restore your essential service.	You have appropriately secured backups (including data, configuration information, software, equipment, processes and key roles or knowledge). These backups will be accessible to recover from an extreme event.	Your comprehensive, automatic and tested technical and procedural backups are secured at centrally accessible or secondary sites to recover from an extreme event.
Backups are not frequent enough for your essential service to be restored within a suitable timeframe.	You routinely test backups to ensure that the backup process functions correctly and the backups are usable.	Key roles are duplicated and operational delivery knowledge is shared with all individuals involved in the operations and recovery of the essential service.
		Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed.

B6 Staff Awareness and Training

Principle

Staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to the security of network and information systems supporting the delivery of essential services.

B6.a Cyber security culture

You develop and pursue a positive cyber security culture.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All of the following statements are true	All the following statements are true
People in your organisation don't understand what they contribute to the cyber security of the essential service.	Your executive management understand and widely communicate the importance of a positive cyber security culture. Positive attitudes, behaviours and expectations are described for your organisation.	Your executive management clearly and effectively communicates the organisation's cyber security priorities and objectives to all staff. Your organisation displays positive cyber security attitudes, behaviours and expectations.
People in your organisation don't know how to raise a concern about cyber security.	All people in your organisation understand the contribution they make to the essential service's cyber security.	People in your organisation are positively recognised for bringing cyber security incidents and issues to light, not reprimanded or ignored.
People believe that reporting issues may get them into trouble.	All individuals in your organisation know who to contact and where to access more information about cyber security. They know how to raise a cyber security issue.	Individuals at all levels in your organisation routinely report concerns or issues about cyber security and are recognised for their contribution to keeping the organisation secure.
Your organisation's approach to cyber security doesn't reflect the way staff work to deliver the essential service. It is perceived by staff as being incompatible with the ability of the organisation to deliver the essential service.		Your management is seen to be committed to and actively involved in cyber security.
		Your organisation communicates openly about cyber security, with any concern being taken seriously.
		People across your organisation participate in cyber security activities and improvements, building joint ownership and bringing knowledge of their area of expertise.

B6.b Cyber security training

The people who operate and support your essential service are appropriately trained in cyber security. A range of approaches to cyber security training, awareness and communications are employed.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All of the following statements are true	All the following statements are true
There are teams in your organisation that do not have at least one individual with full cyber security training in that role.	You have defined appropriate cyber security training and awareness activities for all roles in your organisation, from executives to the most junior roles.	All people in your organisation, from executives to the most junior roles, follow appropriate cyber security training paths.
Cyber security training is only offered to specific roles in your organisation.	You use a range of teaching and communication techniques for cyber security training and awareness to reach the widest audience effectively.	You track individuals' cyber security training and ensure that refresh update training is completed at suitable intervals.
Records of role-specific cyber security training do not exist, or are incomplete.	Cyber security information is easily available.	You routinely engage all people across your organisation on cyber security and evaluate that your cyber security training and awareness activities reach the widest audience effectively.
There are incomplete or no records of cyber security training for your organisation.		Cyber security information and good practice guidance is easily and widely available. You know this is referenced and employed by people in your organisation.

CAF - Objective C - Detecting cyber security events

C1 Security Monitoring

Principle

The organisation monitors the security status of the networks and systems supporting the delivery of essential services in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.

C1.a Monitoring coverage

The data sources that you include in your monitoring allow for timely identification of security events which might affect the delivery of your essential service.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All of the following statements are true	All the following statements are true
You are not collecting data relating to the security and operation of your essential services.	Network data is collected for some areas of the essential service.	You understand, based on your knowledge of your networks and common cyber attack methods, what you need to monitor in order to detect potential security incidents that could affect your essential service. For example, presence of malware, malicious emails, policy violation by a user.
You are not able to apply Indicators of Compromise to systems monitoring your essential services to confidently detect the presence or absence of those IoCs (e.g. because your logging data is not sufficiently detailed).	You are able to look for most IoCs you receive, but may need to adjust logging coverage or data quality to deal with some IoCs.	Your monitoring data provides sufficient detail to reliably detect security incidents that could affect your essential service.
You are not able to audit the activities of users in relation to your essential service.	Some user monitoring is done, but not covering a comprehensive range of user activities that might affect them.	You have timely access to the data you need to use with IoCs.
You are not able to capture any traffic crossing your network boundary (e.g. even IP connections).	You are able to monitor traffic crossing your network boundary (including IP address connections as a minimum).	You are able to monitor user activity extensively in relation to essential services. You can detect policy violations and an agreed list of suspicious or undesirable behaviour.
		As well as your network boundary, your monitoring coverage includes internal and host-based monitoring.

		Your process for bringing new systems on line includes considerations for access to monitoring data sources.

C1.b Securing Logs

Logging data should be held securely and read access to it should be granted only to accounts with business need. No employee should ever need to modify or delete logging data within an agreed retention period, after which it should be deleted.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All of the following statements are true	All the following statements are true
It is possible for logging data to be edited or deleted.	Only certain staff can view logging data for investigations.	The integrity of logging data is protected or any modification is detected and attributed.
There is no controlled list of who can view and query logging information.	Privileged users can view logging information.	Logging data is segregated from the rest of the network, so disruption or corruption to network data does not affect the logging data.
There is no monitoring of the access to logging data.	Some monitoring of access to logging data.	Any alterations to logging data (e.g. re- normalising for SIEM analysis) is done on copies, not the master.
There is no policy for accessing logging data.	Some logging datasets are synchronised.	Logging datasets are synchronised, using a common time source, so separate datasets can be correlated in different ways.
Logging is not synchronised, using an accurate time source.		Access to logging data is limited to those with business need and no others.
		All actions involving all logging data (e.g. copying, deleting or modification, or even viewing) can be traced back to a unique user.
		Legitimate reasons for accessing logging data are given in use policies and users are trained on this.

C1.c Generating alerts

Evidence of potential security incidents contained in your monitoring data is reliably identified and alerted upon.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All of the following statements are true	All the following statements are true
You are not able to investigate alerts provided by 3rd parties e.g. an antivirus (AV) provider.	You are able to investigate AV alerts.	You are able to investigate AV alerts.
Your logging data is stove- piped, stored in different places and difficult to aggregate to investigate alerts.	Some logging datasets are stored centrally and can be used for some investigations.	You are able to aggregate separate datasets to investigate activity or alerts (e.g. by enriching logging data with other network data, or knowledge of the network more generally) and are able to make maximal use of a wide range of signatures and IoCs.
You are not able to use log data to resolve alerts to a network asset or system.	You are able to use log data to resolve alerts to a network asset or system.	You are able to resolve alerts to network assets, using knowledge of the network and systems.
You are not able to flag security alerts that relate to essential services.	You are able to flag alerts that relate to your essential services.	You are able to flag alerts that relate to essential services and use this information to support your incident management capability.
Logs are not reviewed regularly.	Logs are reviewed at regular intervals.	Logs are reviewed almost continuously, in real time.
		You are able to test that alerts are generated reliably and that genuine security incidents are distinguishable from false alarms.

C1.d Identifying security incidents

You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All of the following statements are true	All the following statements are true
Your organisation has no sources of threat intelligence.	Your organisation uses some threat intelligence services, but you don't choose providers specifically because of your business needs, or specific threats in your sector (e.g. sector-based infoshare, ICS software vendors, antivirus providers, specialist threat intel firms).	You have selected threat intelligence feeds using risk-based and threat-informed decisions based on your business needs and sector (e.g. vendor reporting and patching, strong antivirus providers, sector and community-based infoshare).
You do not apply intelligence updates (e.g. AV signature updates, other threat signatures or IoCs) in a timely way, after receiving them.	You apply some updates, signatures and IoCs in a timely way.	You are able to apply new signatures and IoCs within a reasonable (risk-based) time of receiving them.
You do not receive signature updates for all protective technologies (such as AV and IDS) or other software in use.	You receive signature updates for all your protective technologies (e.g. AV, IDS).	You receive signature updates for all your protective technologies (e.g. AV, IDS).
You do not evaluate the usefulness of your threat intelligence or share feedback with providers or other users.	You are cognisant of how effective your threat intelligence is (e.g. by tracking how threat intelligence helps you identify security problems).	You can track the effectiveness of your intelligence feeds and actively share feedback on the usefulness of IoCs and any other indicators with the threat community (e.g. sector partners, threat intelligence providers, government agencies).

C1.e Monitoring tools and skills Monitoring staff skills, tools and roles, including any that are out-sourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential services they need to protect.		
Not Achieved	**Partially Achieved**	**Achieved**
Any of the following statements are true	All of the following statements are true	All the following statements are true
There are no staff who perform a monitoring function.	Monitoring staff have some investigative skills and a basic understanding of the data they need to work with.	You have monitoring staff, who are responsible for investigating and reporting monitoring alerts.
Monitoring staff do not have the correct specialist skills.	Monitoring staff can report to other parts of the organisation (e.g. security directors, resilience managers).	Monitoring staff have roles and skills that covers all parts of the monitoring/investigation workflow.
Monitoring staff are not capable of reporting against governance requirements	Monitoring staff are capable of following most of the required workflows.	Monitoring staff have workflows that address all governance reporting requirements, internal and external.
Monitoring staff lack the skills to successfully perform any part of the defined workflow.	Your monitoring tools can make use of logging that would capture most common attack types.	Monitoring staff are empowered to look beyond fixed workflows to investigate and understand non-standard threats, by developing their own investigative techniques and making new use of data.
Monitoring tools are only able to make use of a fraction of logging data being collected.	Your monitoring staff are aware of some essential services and can manage alerts relating to them.	With some configuration, your monitoring tools are able to make use of all logging data collected.
Monitoring tools cannot be configured to make use of new logging streams, as they come online.		Monitoring staff and tools are able to drive and shape new log data collection and can make wide use of it.
Monitoring staff are not aware of some essential services the organisation provides and what assets (and hence logging data and security events) relate to those services.		Monitoring staff are aware of essential services and related assets and can identify and prioritise alerts or investigations that relate to them.

C2 Proactive Security Event Discovery **Principle** *The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the delivery of essential services, even when the activity evades*

C2.a System abnormalities for attack detection You define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify.	
Not Achieved	**Achieved**
At least one of the following is true	All the following statements are true
Your understanding of normal system behaviour is insufficient to be able to exploit the use of system abnormalities to detect malicious activity,	You have a sufficient understanding of normal system activity (e.g. which system components should and should not be communicating with each other) to ensure that searching for system abnormalities is a potentially effective way of detecting malicious activity.
You have no established understanding of what abnormalities to look for that might signify malicious activities.	You maintain descriptions of some system abnormalities that might signify malicious activity, informed by past attacks (on yours and others' networks), threat intelligence and a general understanding of what an attack might look like.
	Your choice of system abnormalities to search for takes into account the nature of attacks likely to impact on the networks and information systems supporting the delivery of essential services.
	You regularly update the descriptions of the system abnormalities that you search for to reflect changes to your networks and information systems and current threat intelligence.

C2.b Proactive attack discovery You use an informed understanding of more sophisticated attack methods and of normal system behaviour to monitor proactively for malicious activity.	
Not Achieved	**Achieved**
At least one of the following is true	All the following statements are true
You do not routinely search for system abnormalities indicative of malicious activity.	You routinely search for system abnormalities indicative of malicious activity with the potential to have an impact on networks and information systems supporting your essential service, and you generate alerts based on the results of such searches.
	You have justified confidence in the effectiveness of your searches for system abnormalities.

CAF - Objective D - Minimising the impact of cyber security incidents

D1 Response and Recovery Planning

Principle

There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential services in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.

D1.a Response plan

You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of your essential service and covers a range of incident scenarios.

Not Achieved	Partially Achieved	Achieved
At least one of the following is true		All the following statements are true
Your incident response plan is not documented.	Your response plan covers your essential services.	Your incident response plan is based on a clear understanding of the security risks to the networks and information systems supporting your essential service.
Your incident response plan does not include your organisation's identified essential service.	Your response plan comprehensively covers scenarios that are focused on likely impacts of known and well- understood attacks only.	Your incident response plan is comprehensive (i.e. covers the complete lifecycle of an incident, roles and responsibilities, and reporting) and covers likely impacts of both known attack patterns and of possible attacks, previously unseen.
Your incident response plan is not well understood by relevant staff.	Your response plan is understood by all staff who are involved with your organisation's response function.	Your incident response plan is documented and integrated with wider organisational business and supply chain response plans.
	Your response plan is documented and shared with all relevant stakeholders.	Your incident response plan is communicated and understood by the business areas involved with the supply or maintenance of your essential services.

D1.b Response and recovery capability

You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.

Not Achieved	Achieved
At least one of the following is true	All the following statements are true
Inadequate arrangements have been made to make the right resources available to implement your response plan.	You understand the resources that will likely be needed to carry out any required response activities, and arrangements are in place to make these resources available.
Your response team members are not equipped to take good response decisions and put them into effect.	You understand the types of information that will likely be needed to inform response decisions and arrangements are in place to make this information available.
Inadequate back-up mechanisms exist to allow the continued delivery of your essential service during an incident.	Your response team members have the skills and knowledge required to decide on the response actions necessary to limit harm, and the authority to carry them out.
	Back-up mechanisms are available that can be readily activated to allow continued delivery of your essential service (although possibly at a reduced level) if primary networks and information systems fail or are unavailable.
	Where necessary, arrangements are in place to augment your organisation's incident response capabilities with external support (e.g. specialist providers of cyber incident response capability).

D1.c Testing and exercising

Your organisation carries out exercises to test response plans, using past incidents that affected your (and other) organisation, and scenarios that draw on threat intelligence and your risk assessment.

Not Achieved	Achieved
At least one of the following is true	All the following statements are true
Exercises test only a discrete part of the process (e.g. that backups are working), but do not consider all areas.	Exercise scenarios are based on incidents experienced by your and other organisations, or are composed using experience or threat intelligence.
Incident response exercises are not routinely carried out, or are carried out in an ad-hoc way.	Exercise scenarios are documented, regularly reviewed, and validated.
Outputs from exercises are not fed into the organisation's lessons learned process.	Exercises are routinely run, with the findings documented and used to refine incident response plans and protective security, in line with the lessons learned.
Exercises do not test all parts of the response cycle.	Exercises test all parts of your response cycle relating to particular services or scenarios (e.g. restoration of normal service levels).

D2 Lessons Learned

Principle

When an incident occurs, steps are taken to understand its root causes and ensure appropriate remediating action is taken to protect against future incidents.

D2.a Incident root cause analysis Your organisation identifies the root causes of incidents you experience, wherever possible.	
Not Achieved	**Achieved**
At least one of the following is true	**All the following statements are true**
You are not usually able to resolve incidents to a root cause.	Root cause analysis is conducted routinely as a key part of your lessons learned activities following an incident.
You do not have a formal process for investigating causes.	Your root cause analysis is comprehensive, covering organisational process issues, as well as vulnerabilities in your networks, systems or software.
	The incident data that is necessary to undertake incident root cause analysis is available to the analysis team.

D2.b Using incidents to drive improvements Your organisation uses lessons learned from incidents to improve your security measures.	
Not Achieved	**Achieved**
At least one of the following is true	**All the following statements are true**
Following incidents, lessons learned are not captured or are limited in scope.	You have a documented incident review process/policy which ensures that lessons learned from each incident are identified, captured, and acted upon.
Improvements arising from lessons learned following an incident are not implemented or not given sufficient organisational priority.	Lessons learned cover issues with reporting, roles, governance, skills and organisational processes as well as technical aspects of networks and information systems.
	You use lessons learned to improve security measures, including updating and retesting response plans when necessary.
	Security improvements identified as a result of lessons learned are prioritised, with the highest priority improvements completed quickly.

Tripwire Product Mapping Against the NIS Directive Cyber Assessment Framework (CAF)

Objective A: Managing Security Risk					
Principle A1 - Governance					
A1.a	Board Direction	NA			
A1.b	Roles & Responsibilities	NA			
A1.c	Decision Making	NA			
Principle A2 - Risk Management					
A2.a	Risk Management Process	Partially Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility
A2.b	Assurance	Partially Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility
Principle A3 - Asset Management					
A3.a	Asset Management	Partially Achieved			Tripwire Industrial Visibility
Principle A4 - Supply Chain					
A4.a	Supply Chain	NA			
Objective B: Protecting against Cyber-attack					
Principle B1 - Service protection policies and processes					
B1.a	Policy and process development	NA			
B1.b	Policy and Process Implementation	NA			
Principle B2 - Identity and Access Control					
B2.a	Identity Verification, Authentication and Authorization	NA			
B2.b	Device Management	Partially Achieved			Tripwire Industrial Visibility
B2.c	Privileged User Management	NA			
B2.d	IDAC Management and Maintenance	NA			
Principle B3 - Data Security					
B3.a	Understanding Data	Partially Achieved	Tripwire Enterprise		Tripwire Industrial Visibility
B3.b	Data in Transit	Partially Achieved			Tripwire Industrial Visibility
B3.c	Stored Data	Partially Achieved	Tripwire Enterprise		
B3.d	Mobile Data	Partially Achieved			Tripwire Visibility
B3.e	Media / Equipment Sanitization	NA			
Principle B4 - System Security					
B4.a	Secure by Design	Partially Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility
B4.b	Secure Configuration	Partially Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility
B4.c	Secure Management	Partially Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility
B4.d	Vulnerability Management	Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility
Principle B5 - Resilient Networks and Systems					
B5.a	Resilience Preparation	Partially Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility

B5.b	Design for Resilience	Partially Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility
B5.c	Backups	NA			

Principle B6 - Staff Awareness and Training

B6.a	Cyber Security Culture	Partially Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility
B6.b	Cyber Security Training	Partially Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility

Objective C: Detecting Cyber Security Events

Principle C1 - Security Monitoring

C1.a	Monitoring Coverage	Partially Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility
C1.b	Security Logs	Partially Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility
C1.c	Generating Alerts	Partially Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility
C1.d	Identifying Security Incidents	Partially Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility
C1.e	Monitoring Tools and Skills	Partially Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility

Principle C2 - Proactive Security Event Discovery

C2.a	System Abnormalities for Attack Detection	Partially Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility
C2.b	Proactive Attack Discovery	Partially Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility

Objective D: Minimizing the Impact of Cyber Security Incidents

Principle D1 - Response and Recovery Planning

D1.a	Response Plan	Partially Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility
D1.b	Response and Recovery Capability	Partially Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility
D1.c	Testing and Exercising	Partially Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility

Principle D2 - Lessons Learned

D2.a	Incident Root Cause Analysis	Partially Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility
D2.b	Using Incidents to Drive Improvements	Partially Achieved	Tripwire Enterprise	Tripwire IP360	Tripwire Industrial Visibility

Tripwire Product Mapping — Rationalization

Objective A: Managing Security Risk					
Principle A1 - Governance					
A1.a	Board Direction	NA			
A1.b	Roles & Responsibilities	NA			
A1.c	Decision Making	NA			
Principle A2 - Risk Management					
A2.a	Risk Management Process	Partially Achieved	TE: Product will provide risk reduction and mitigation against identified changes and compliance assurance across the ICS / OT environment.	TIP: Product will provide risk reduction and mitigation against identified vulnerabilities and will provide this on a continuous basis upon periodic scanning of the ICS / OT environment.	TIV: Product will provide risk reduction and mitigation against identified changes and rouge devices within the environment via the passive scanning process on a continuous basis.
A2.b	Assurance	Partially Achieved	TE: Product will enable the assurance testing of the security controls being implemented. - Report generation will provide the audit mechanism to ensure full traceability of assurance testing.	TIP: Product will enable the assurance testing of the security controls being implemented. - Report generation will provide the audit mechanism to ensure full traceability of assurance testing.	TIV: Product will enable the assurance testing of the security controls being implemented. - Report generation will provide the audit mechanism to ensure full traceability of assurance testing.
Principle A3 - Asset Management					
A3.a	Asset Management	Partially Achieved			TIV: Product will provide the identification of all systems and components to ensure the asset management and base line controls can be adhered too. Prioritization exercise would still be required in-order to determine the order of reconstitution order of the critical systems / components.
Principle A4 - Supply Chain					
A4.a	Supply Chain	NA			
Objective B: Protecting against Cyber-attack					
Principle B1 - Service protection policies and processes					
B1.a	Policy and process development	Partially Achieved	Policy can be defined within the products to map against the policy defined by the customers / organization – reporting against non-compliance on a periodic basis combined with the resolution / mitigation process can provide a road-map.		
B1.b	Policy and Process Implementation	NA	Policy and process implementation would be covered as part of the policy development - implementation of this policy (set of controls).		
Principle B2 - Identity and Access Control					
B2.a	Identity verification, authorization and authorization	NA			

Note:

TE = Tripwire® Enterprise

TIP = Tripwire IP360™

TIV = Tripwire Industrial Visibility

TLC = Tripwire LogCenter®

B2.b	Device Management	Partially Achieved			TIV: Product will enable the device management principles by ensuring the identification of all assets across the ICS / OT environment. Understanding of all component aspects and constant configuration checking will provide key aspects in CMD.
B2.c	Privileged User Management	NA			
B2.d	IDAC Management and Maintenance	NA			
Principle B3 - Data Security					
B3.a	Understanding Data	Partially Achieved	TE: Understanding what data resides within th ICS / OT environment is vital, being able to apply the correct security controls against that identified critical data is what FIM will provide - FIM against Databases / Active Directory / Critical Files (Process / Account Data / Configuration).		TIV: Product will enable the user to realize the data communication flows between the systems / components – realization of the data flows and being able to map this will provide significant understanding as to the where and why.
B3.b	Data in Transit	Partially Achieved			TIV: Product will enable the user to realize the data communication flows between the systems / components – realization of the data flows and being able to map this will provide significant understanding as to the where and why.
B3.c	Stored Data	Partially Achieved		TIP: Product will enable the user to provide FIM to critical files etc.	
B3.d	Mobile Data	Partially Achieved			TIV: Product will enable the user to cataloged and understood the mobile devices used for essential services
B3.e	Media / Equipment Sanitization	NA			
Principle B4 - System Security					
B4.a	Secure by Design	Partially Achieved	TE: Product will provide the identified functionality to enabling a secure design: - Asset Identification & change control / notification - Data Security - Device Management - Asset Management - Security Monitoring - Proactive Security Event Discovery	TIP: Product will provide the identified functionality to enabling a secure design: - Asset Identification & sub-component details via vulnerability scanning - Data Security - Device Management - Asset Management - Security Monitoring - Proactive Security Event Discovery	TIV: Product will provide the identified functionality to enabling a secure design: - Asset Identification & Prioritization - Data Security - Device Management - Asset Management - Security Monitoring - Proactive Security Event Discovery
B4.b	Secure Configuration	Partially Achieved	All products will increase the overall security configuration for systems / components within the ICS / OT environment – the identification / monitoring and event alerting will ensure the assets are constantly being reviewed against the ever increasing threat landscape.		
B4.c	Secure Management	Partially Achieved	All products will increase the overall security management for systems / components within the ICS / OT environment – the identification / monitoring and event alerting will ensure the assets are constantly being reviewed against the ever increasing threat landscape.		

B4.d	Vulnerability Management	Achieved		TIP: Product provides complete vulnerability management, identification and alerting against vulnerabilities identified across the ICS / OT environment.	

Principle B5 - Resilient Networks and Systems

B5.a	Resilience Preparation	Partially Achieved	All products can be configured to ensure the security services for the ICS / OT environment can be reconstituted within the specified SLA - provision of High Availability (HA) aspects within a virtual platform can be achieved.
B5.b	Design for Resilience	Partially Achieved	All products can be designed and commissioned to ensure the resilience of the security services for the ICS / OT environment can be achieved.
B5.c	Backups	NA	All products will provision backups of internal configurations and imagery to ensure the reconstitution of the security services within the ICS / OT environment can be achieved with the specified SLA.

Principle B6 - Staff Awareness and Training

B6.a	Cyber Security Culture	Partially Achieved	Not direct - deployment of security products and the management life-cycle improves the cyber security culture within the team and across the organization.
B6.b	Cyber Security Training	Partially Achieved	All products offer proven / accredited training programs - offerings provide maintainers with the tools and skill sets to manage and maintain the products within the ICS / OT environment.

Objective C: Detecting Cyber Security Events

Principle C1 - Security Monitoring

C1.a	Monitoring Coverage	Partially Achieved	TE: Product will provide File Integrity Monitoring (FIM) alerting of critical files within the ICS / OT environment	TIP: Product will provide vulnerability management, identification and alerting of those systems / components within the ICS / OT infrastructure being identified with current vulnerabilities.	TIV: Product will provide monitoring of systems and components across all levels within the Purdue Model depending on the placement of the data collectors.
C1.b	Security Logs	Partially Achieved	TE: Product can provision secure logging capability with own components or to a centralized SIEM solution in order to enhance the capability of security monitoring. Ability to provide logging against change management within the ICS / OT environment TLC: Coverage with Tripwire LogCenter	TIP: Product can provision secure logging capability with own components or to a centralized SIEM solution in order to enhance the capability of security monitoring TLC: Coverage with Tripwire LogCenter	TIV: Product can provision secure logging capability with own components or to a centralized SIEM solution in order to enhance the capability of security monitoring TLC: Coverage with Tripwire LogCenter
C1.c	Generating Alerts	Partially Achieved	TE: Product can generate alerts within own components or to a centrally managed SIEM. TLC: Coverage with Tripwire LogCenter	TIP: Product can generate alerts within own components or to a centrally managed SIEM. TLC: Coverage with Tripwire LogCenter	TIV: Product can generate alerts within own components or to a centrally managed SIEM. TLC: Coverage with Tripwire LogCenter
C1.d	Identifying Security Incidents	Partially Achieved	TE: Product can identify the change and sequence of critical files within the ICS / OT environment. TLC: Product will provide data forensic capability for incident response	TIP: Product can identify the status of those given systems and components as part of the scanning process, vulnerabilities can be identified and categorized. TLC: Product will provide data forensic capability for incident response	TIV: Product can identify security incidents such as the initiation of a rouge device being plugged into the ICS / OT environment. TLC: Product will provide data forensic capability for incident response

C1.e	Monitoring Tools and Skills	Partially Achieved	TE: The use of advanced software tools within the security field provide for the combination of multi vendor security products and the use of providing the security events to a centrally managed SIEM in order for the event correlation to be analyzed and actioned. TLC: Use of Tripwire LogCenter to provide analytics	TIP: The use of advanced software tools within the security field provide for the combination of multi vendor security products and the use of providing the security events to a centrally managed SIEM in order for the event correlation to be analyzed and actioned. TLC: Use of Tripwire LogCenter to provide analytics	TIV: The use of advanced software tools within the security field provide for the combination of multi vendor security products and the use of providing the security events to a centrally managed SIEM in order for the event correlation to be analyzed and actioned. TLC: Use of Tripwire LogCenter to provide analytics

Principle C2 - Proactive Security Event Discovery

C2.a	System Abnormalities for Attack Detection	Partially Achieved	TE: The identification of change management and FIM will enable the detection of an attack within the ICS / OT environment, changing of critical files by an adversary to escalate privileges etc. will be detected and alerted.	TIP: The identification of vulnerabilities across the environment will reduce attack vectors.	TIV: The provision of an asset identification and data flow analysis provides a base line of the ICS / OT environment, this can be utilized as the detection of change within that environment.
C2.b	Proactive Attack Discovery	Partially Achieved	All products will provide attack discovery: TE - will provide notification of changes within the ICS / OT environment TIP - will provide the vulnerability identification across systems / components TIV - will provide the analysis across the network to discover rouge devices / components TLC - will provide log storage and management for forensic capability post attack		

Objective D: Minimizing the Impact of Cyber Security Incidents

Principle D1 - Response and Recovery Planning

D1.a	Response Plan	Partially Achieved	Not direct – all products will add to the response planning of the organization.
D1.b	Response and Recovery Capability	Partially Achieved	Not direct – all products will add to the response and recovery capability of the ICS / OT environment.
D1.c	Testing and Exercising	Partially Achieved	Not direct – all products will be part of the testing and exercising of the attack vectors and be part of the red / blue team exercising.

Principle D2 - Lessons Learned

D2.a	Incident Root Cause Analysis	Partially Achieved	All products will enable the data reporting / forensic capability in order to determine the root cause investigation and analysis of a security incident - this combined with the full audit capability in which Tripwire products have implemented will ensure the identification of the internal / insider threat.
D2.b	Using Incidents to Drive Improvements	Partially Achieved	Not direct – all products will provide aspects of being able to drive improvements within the organization.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

MXNIS1b2 1906