FORESCOUT

Cyber Assessment Framework Matrix

Cyber Assessment Framework Objective A

A1 Governance		
Description	Appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to the network and information systems supporting essential services.	
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**	**How Forescout can help**
At least one statement is true	All 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. Board-level discussions on the security of networks and information systems are based on partial or out-of-date information, without the benefit of expert guidance. The security of networks and information systems supporting your essential services is not driven effectively by the direction set at board level. Senior management or other pockets of the organisation consider themselves exempt from some policies, or expect special accommodations to be made.	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. 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. 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. 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.	**Not Applicable to Technical Tools like Forescout**

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**	**How Forescout can help**
At least one of the following statements is true	All the following statements is true	
Key roles are missing, left vacant, or fulfilled on an ad-hoc or informal basis. Staff are assigned security responsibilities but without adequate authority or resources to fulfil them. Staff are unsure what their responsibilities are for the security of the essential service.	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. Appropriately capable and knowledgeable staff fill those roles and are given the time, authority, and resources to carry out their duties. There is clarity on who in your organisation has overall accountability for the security of the networks and information systems supporting your essential service.	**Not Applicable to Technical Tools like Forescout**

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**	**How Forescout can help**
At least one statement is true	All statements are true	
What should be relatively straightforward risk decisions are constantly referred up the chain, or not made. Risks are resolved informally (or ignored) at a local level without a formal reporting mechanism when it is not appropriate. Decision-makers are unsure of what senior management's risk appetite is, or only understand it in vague terms such as "averse" or "cautious".	Senior management have visibility of key risk decisions made throughout the organisation. 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. 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.	**Not Applicable to Technical Tools like Forescout**

A1.c Decision-making (continued)		How Forescout can help
Not Achieved	**Achieved**	
At least one statement is true	All statements are true	
Organisational stovepipes result in risk decisions being made in isolation, for example, engineering and IT don't talk to each other about risk. Risk priorities are too vague to make meaningful distinctions between them, for example almost all risks are rated 'medium' or 'amber'.	Risk management decisions are periodically reviewed to ensure their continued relevance and validity.	**Not Applicable to Technical Tools like Forescout**

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 risk management.	
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. delivery of essential services are considered in the context of other organisational risks.	
Not Achieved	**Achieved**	**How Forescout can help**
At least one statement is true	All statements are true	
Risk assessments are not based on a clearly defined set of threat assumptions. 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. Risk assessments for critical systems are a "one-off" activity (or not done at all). The security element of project or programme milestones are solely dependent on completing the risk management process. One single approach to assessing risks is applied to every risk management problem within the organisation.	Your organisational process ensures that security risks to networks and information systems relevant to essential services are identified, analysed, prioritised, and managed. 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. 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.	**Forescout's ability to see and control managed and unmanaged devices, including IoT devices on a network reduces the risk of potential attacks and remediates malicious code or high-risk devices**

A2.a Risk management process (continued)

Not Achieved	Achieved	How Forescout can help
At least one statement is true	All statements are true	
Systems are assessed in isolation, without consideration of dependencies and interactions with other systems (including interactions between IT and OT environments). 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. Risks remain unresolved on a register for prolonged periods of time awaiting senior decision-making or resource allocation to resolve.	Your risk assessments are informed by an understanding of the vulnerabilities in the networks and information systems supporting your essential service. 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 Significant conclusions reached in the course of your risk management process are communicated to key security decision-makers and accountable individuals. 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 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	How Forescout can help
At least one statement is true	All statements are true	
A particular product or service is seen as a “silver bullet” and vendor claims are taken at face value. Assurance methods are applied without appreciation of their strengths and limitations, such as the risks of penetration testing in operational environments. Assurance is assumed because there have been no known problems to date.	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. You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of essential services. Your confidence in the security as it relates to your technology, people, and processes can be demonstrated to, and verified by, a third party.	**Not Applicable to Technical Tools like Forescout**

A2.b Assurance (continued)		
Not Achieved	**Achieved**	**How Forescout can help**
At least one statement is true	All statements are true	
	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 supporting infrastructure (such as power or cooling).

A3.a Asset management		
Not Achieved	**Achieved**	**How Forescout can help**
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. 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). 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. Knowledge critical to the management, operation, or recovery of essential services is held by one or two key individuals with no succession plan. Asset inventories are neglected and out of date.	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. Dependencies on supporting infrastructure (eg. power, cooling etc) are recognised and recorded. You have prioritised your assets according to their importance to the delivery of the essential service. You have assigned responsibility for managing the physical assets. Assets relevant to essential services are managed with cyber security in mind throughout their lifecycle, from creation through to eventual decommissioning or disposal.	**Not Applicable to Technical Tools like Forescout**

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 suppliers. This includes ensuring that appropriate measures are employed where third party services are used. Regardless of your outsourcing model the OES remains responsible for the security of the service and therefore all requirements from NIS flow down.		
A4.a Supply chain			
Not Achieved	**Partially Achieved**	**Achieved**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
You do not know what data belonging to you is held by suppliers, or how it is managed. Elements of the supply chain for essential services are subcontracted and you have little or no visibility of the sub-contractors. Relevant contracts do not have security requirements. Suppliers have unrestricted or unmonitored access to critical systems, or access that bypasses your own security controls.	You understand the general risks suppliers may pose to your essential services. You know the extent of your supply chain for essential services, including sub-contractors. You engage with suppliers about security, and you set and communicate security requirements in contracts. You are aware of all third-party connections and have assurance that they meet your organisation's security requirements. Your approach to security incident management considers incidents that might arise in your supply chain.	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. 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. You have confidence that information shared with suppliers that might be essential to the service is well protected. 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. All network connectivity and data object exchange is appropriately managed. Where appropriate, you offer support to suppliers to resolve incidents.	**The Forescout platform can continuously acquire, assess and take action on new information in order to identify vulnerabilities, remediate noncompliant or compromised devices and minimize the window of opportunity for attackers.**

Cyber Assessment Framework Objective B

B1 Service Protection Policies and Processes

Description	Proportionate security measures in place to protect essential services and systems from cyber attack.
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 processes 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	How Forescout can help
At least one statement is true	All statements are true	All statements are true	
Your service protection policies and processes are absent or incomplete. Service protection policies and processes are not applied universally or consistently. People often or routinely circumvent service protection policies and processes to achieve business objectives. Your organisation's security governance and risk management approach has no bearing on your service protection policies and processes. System security depends upon users' careful and consistent application of manual security processes. 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.	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 review and update service protection policies and processes in response to major cyber security incidents.	You document your overarching security governance and risk management approach, technical security practiceand specific regulatory compliance. Cyber security is embedded throughout these policies and processes and key performance indicators are reported to your executive management. Your organisation's service protection policies and processes are developed to be practical, usable and appropriate for your essential service and your technologies. 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. 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. Your systems are designed with 'guard rails', so that they remain secure even when user security policies and processes are not always followed.	**The Forescout platform offers the unique ability to see devices the instant they connect to your network, without requiring software agents or previous device knowledge. It profiles and classifies devices, users, applications and operating systems while continuously monitoring managed devices, personally owned devices and other endpoints, as well as ports and connections. Centrally administered, it can dynamically manage up to 2 million devices in a single Enterprise Manager deployment.**

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**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
None or only part of your service protection policies and processes are enacted. You do not have an understanding of the impact of your service protection policies and processes on your security.	All your service protection policies and processes are enacted and you assess their correct application. Your service protection policies and processes are integrated with other organisational policies and processes, including HR assessments of individuals' trustworthiness. All staff are aware of their responsibilities under your 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.	All your service protection policies and processes are enacted. You regularly evaluate the correct application and security effectiveness of your service protection policies. 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 effectively and appropriately communicated across all levels of the organisation. All staff are aware of their responsibilities under your service protection policies and processes. Suitable action is taken to correct significant single or aggregated breaches of service protection policies and processes.	**The Forescout platform can help with continuous compliance by:** • **Monitoring and detecting authorized and unauthorized wireless access points connected to the CNI network.** • **Monitoring and detecting authorized and unauthorized wireless access points connected to the PCI network.** • **Creating policies to automatically isolate rogue access points, as well as notifying personnel of discoveries.** • **Helping to ensure real-time vulnerability scan compliance with various third-party vulnerability scanners.** • **Performing vulnerability scans for endpoints and networks determined by policy.** • **Detecting malicious activity and integrating with third-party advanced threat detection and SIEM systems.**

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, authenticate and authorise access to the networks and information systems supporting your essential service		
Not Achieved	**Partially Achieved**	**Achieved**	**How Forescout can help**
At least one statements is true	All statements are true	All 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. Unknown or unauthorised users or devices can connect to your networks or information systems. User access is not limited to the minimum necessary. Some or all staff are unaware of their responsibilities under your service protection policies and processes. You do not detect breaches of service protection policies and processes.	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. User access to essential service networks and information systems is 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 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.	Only individually authenticated and authorised users can connect to or access your networks or information systems. Both logical and physical accessrequire this individual authentication and authorisation. User access to all your networks and information systems supporting the essential service is limited to the minimum necessary. You use additional authentication mechanisms, such as two-factor or hardware-backed certificates, for all systems that operate or 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 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.	**The Forescout platform identifies users attempting to access information they are not authorized access to by their Active Directory group. It provides device- and role-based network authentication and authorization, allowing individuals and their devices to get their identified network access determined by VLANs or ACLs.**

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**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
Users are allowed to connect to your essential service's networks using personal devices. Administrators are able to perform administrative functions from non-corporately managed devices (such as remote access from personal devices). You have not gained assurance in the security of any third-party devices or networks connected to your systems. Physically connecting to your network gives a device access to systems without further authentication.	Only enterprise-owned and managed devices are allowed to access your essential service's networks and information systems. All administrative access occurs from dedicated management devices. 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. The act of connecting to a network port or cable does not grant access to any systems. You are able to detect unknown devices being connected to your network, and investigate such incidents.	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. 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 perform device identity management which is cryptographically backed, and only allow known devices to access systems. You perform regular scans to detect unknown devices and investigate any findings.	**The Forescout platform can help ensure that relevant third-party protection software is installed, correctly configured and operational. Connecting devices can be evaluated as part of Forescout's access inspection, and non-conforming hosts can be quarantined or removed from the network until repaired. It can identify open ports, active protocols and services currently running, and compare that inventory with configuration policies for that host. It can also restrict or deny access for noncompliant devices and issue a user notification or remediation alert.**

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**	**How Forescout can help**
At least one statement is true	All statements are true	All 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.	**The Forescout platform can deliver real-time enforcement of policies for non-privileged and privileged accounts.**

B2.c Privileged user management (continued)

Not Achieved	Partially Achieved	Achieved	How Forescout can help
At least one statement is true	All statements are true	All statements are true	
It is not known whether all privileged users are strongly authenticated when accessing the system. Privileged access is granted from remote sessions without additional validation. The list of system administrators has not been reviewed recently, e.g. within the last 12 months. Privileged user access is granted on a system-wide basis (as opposed to by specific roles). System administrators use generic (shared or default name) accounts to administer servers and devices. 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. 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 know the names of all individuals in your organisation and your supply chain with privileged access to your networks and information systems (infrastructure, platforms, software, configuration, etc.) Activity by privileged users is periodically validated, e.g. annually. Privileged users are only granted specific privileged permissions and roles which are essential to their business function.	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. You regularly review privileged access rights and always update privileges as part of your joiners, movers and leavers process. 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 access is only granted on devices owned and managed by your organisation. Activity by privileged users is routinely validated. The list of system administrators is regularly reviewed, e.g. every 6 months. 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 for your networks and information systems supporting the essential service. You closely manage privileged user access to networks and information systems supporting the essential service.		
Not Achieved	**Partially Achieved**	**Achieved**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
Greater rights are granted to users than necessary. User rights are granted without validation of their identity and requirement for access. User rights are not reviewed when they move jobs. User rights remain active when people leave your organisation.	You have a robust procedure to verify each user and issue minimum required access rights. You regularly review access rights and those no longer needed are revoked. 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.	You have an auditable, robust procedure to verify each user and issue minimum required access rights. Your joiners, leavers and movers process ensures that, in addition to when people change roles, user permissions are reviewed regularly. 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.	**The Forescout platform provides critical capabilities for enforcing access control:** • **Enables limitation of access to information systems to authorized users, processes administered on behalf of authorized users or specified devices/information systems.** • **Can integrate with a variety of third-party authentication systems to validate unique identity and users prior to providing role-based network access.** • **For managed devices, Forescout can identify the users currently logged in and their account types. It compares these with policies for the device and user. If discrepancies are found, Forescout can restrict or deny access.** • **When a remote device requests a network connection, Forescout's initial scan can identify the type of connection and restrict or deny access if the endpoint posture is compromised. At the same time, it can evaluate the device configuration, installed software and patch levels for compliance with security policy.**

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 the delivery of essential services. It also covers information that would assist an attacker, such as design details of networks and information systems.		
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**	**How Forescout can help**
At least one statement is true	All statements are true	All 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 cannot identify who has access to 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 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 periodically review location, transmission, quantity and quality of data important to the delivery of the essential service. You have identified all mobile devices and media that hold data important to the delivery of the essential service. 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 validate these impact statements regularly, e.g. every 12 or 24 months.	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 maintain a current understanding of the location, quantity and quality of data important to the delivery of the essential service. You take steps to remove or minimise unnecessary copies or unneeded historic data. You have identified all mobile devices and media that may hold data important to the delivery of the essential service. 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.	**The Forescout platform helps to protect systems from unauthorized access from untrusted networks:** • **Provides a list of open ports on servers.** • **Identifies traffic attempts from any control / data zone outside of the DMZ.** • **Restricts user and device access using device- and role-based access control.** • **Denies access and/or quarantines endpoints attempting to access the network without personal firewall software installed and functional.**

B3.a Understanding data (continued)			
Not Achieved	**Partially Achieved**	**Achieved**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
		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**	**How Forescout can help**
At least one statement is true	All statements are true	All 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. Data important to the delivery of the essential service travels without technical protection over untrusted or openly accessible carriers. Critical data paths that could fail, be jammed, be overloaded, etc. have no alternative path.	You have identified and suitably protected all the data links that carry data important to the delivery of the essential service. 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 have identified and suitably protected all the data links that carry data important to the delivery of the essential service. 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. 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).	**Forescout's CounterACT platform enables automated segmentation of network access by user, device classification and/or posture, regardless of how that device is connecting to the network—wired, wireless or VPN. Network segregation strategies can be deployed centrally through the Forescout platform**

B3.c Stored data	You have protected stored data important to the delivery of the essential service.		
Not Achieved	**Partially Achieved**	**Achieved**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
You have no, or limited, knowledge of where data important to the delivery of the essential service is stored. You have not protected vulnerable stored data important to the delivery of the essential service in a suitable way. Backups are incomplete, untested, not adequately secured or could be inaccessible in a disaster recovery or business continuity situation.	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 applied suitable physical or technical means to protect this important stored data from unauthorised access, modification or deletion. If cryptographic protections are used, you apply suitable techical and procedural means, but you have limited or no 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 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 applied suitable physical or technical means to protect this important stored data from unauthorised access, modification or deletion. If cryptographic protections are used you apply suitable techical 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.	**As detailed above**

B3.d Mobile data	You have protected data important to the delivery of the essential service on mobile devices.		
Not Achieved	**Partially Achieved**	**Achieved**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
You don't know which mobile devices may hold data important to the delivery of the essential service. 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.	You know which mobile devices hold data important to the delivery of the essential service. Data important to the delivery of the essential service is only stored on mobile devices with at least equivalent security standard to your organisation.	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.	**Not Applicable to Technical Tools like Forescout**

B3.d Mobile data (continued)

Not Achieved	Partially Achieved	Achieved	How Forescout can help
At least one statement is true	All statements are true	All statements are true	
Data on mobile devices is not technically secured, or only some is secured.	Data on mobile devices is technically secured.	Your organisation can remotely wipe all mobile devices holding data important to the delivery of essential service. 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	How Forescout can help
At least one statement is true	All statements are true	
Inventories of assets relevant to the essential service are incomplete, non-existent, or inadequately detailed. 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). 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. Knowledge critical to the management, operation, or recovery of essential services is held by one or two key individuals with no succession plan. Asset inventories are neglected and out of date.	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. Dependencies on supporting infrastructure (eg. power, cooling etc) are recognised and recorded. You have prioritised your assets according to their importance to the delivery of the essential service. You have assigned responsibility for managing the physical assets. Assets relevant to essential services are managed with cyber security in mind throughout their lifecycle, from creation through to eventual decommissioning or disposal.	**Real-time visibility of endpoint agent-based controls, patching and configuration with orchestration capabilities to remediate automatically or initiate a remediation process.** • **Complements agent-based security with its agentless approach. The Forescout platform is infrastructureagnostic and provides real-time visibility into configuration status and gaps for all network infrastructure independent of vendor.** • **Can validate that other security-tool-related processes are complete and compliant with policy, such as vulnerability management, logging and more.** • **Real-time visibility into endpoint- and network-based controls aligns with NIS and other frameworks.**

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**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
Systems essential to the operation of the essential service are not appropriately segregated from other systems. Internet access is available from operational systems. 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. Remote or third party accesses circumvent some network controls to gain more direct access to operational systems of the essential service.	You employ appropriate expertise to design network and information systems. You design strong boundary defences where your networks and information systems interface with other organisations or the world at large. You design simple data flows between your networks and information systems and any external interface to enable effective monitoring. You design to make network and information system recovery simple. 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.	You employ appropriate expertise to design network and information systems. 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. The networks and information systems supporting your essential service are designed to have simple data flows between components to support effective security monitoring. The networks and information systems supporting your essential service are designed to be easy to recover. 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.	**The Forescout platform offers the unique ability to see devices the instant they connect to your network, without requiring software agents or previous device knowledge. It profiles and classifies devices, users, applications and operating systems while continuously monitoring managed devices, personally owned devices and other endpoints, as well as ports and connections. Centrally administered, it can dynamically manage up to 2 million devices in a single Enterprise Manager deployment.**

B4.b Secure configuration	You securely configure the network and information systems that support the delivery of essential services.		
Not Achieved	**Partially Achieved**	**Achieved**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
You haven't identified 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. Configuration details are not recorded or lack enough information to be able to rebuild the system or device. You don't record changes or adjustments to security configuration at security boundaries with the networks and information systems supporting your essential service.	You have identified and documented the assets that need to be carefully configured to maintain the security of the essential service. Secure platform and device builds are used across the estate. Consistent, secure and minimal system and device configurations are applied across the same types of environment. Changes and adjustments to security configuration at security boundaries with the networks and information systems supporting your essential service are approved and documented. You verify software before installation is permitted.	You have identified, documented and actively manage the assets that need to be carefully configured to maintain the security of the essential service. All platforms conform to your secure, consistent baseline build, or latest known good configuration version for that environment. You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented. You regularly review and validate that your network and information systems have the expected, secured settings and configuration. 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.	**The Forescout platform lets you identify missing patches on your endpoints and servers using a combination of native support and module configuration. You can then orchestrate resolution through a number of tools. To help ensure that system components have the necessary patches,** **The Forescout platform can:** • **Identify endpoints without the latest known security patches and quarantine them until patched.** • **Identify traffic attempts between PCI Development, Test and Production Zones.** • **Segregate these environments by enforcing roles-based access.** • **Identify unauthorized user access to servers based on their Active Directory group.**

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**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
Essential service networks and systems are administered or maintained using non-dedicated devices. You do not have good or current technical documentation of your networks and information systems.	Your systems and devices supporting the delivery of the essential service are only administered or maintained by authorised privileged users from dedicated devices. Technical knowledge about networks and information systems, such as documentation and network diagrams, is regularly reviewed and updated. You prevent, detect and remove malware or unauthorised software. You use technical, procedural and physical measures as necessary.	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 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.	**Integration with privileged account management (PAM) systems provides real-time agentless visibility into undiscovered local privileged accounts in the CNI infrastructure and automated response to threats based on holistic visibility into user activity. The Forescout platform can help ensure that relevant third-party protection software is installed, correctly configured and operational.** **Connecting devices can be evaluated as part of Forescout's access inspection, and non-conforming hosts can be quarantined or removed from the network until repaired. It can identify open ports, active protocols and services currently running, and compare that inventory with configuration policies for that host. It can also restrict or deny access for noncompliant devices and issue a user notification or remediation alert.**

B4.d Vulverability management	You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service.		
Not Achieved	**Partially Achieved**	**Achieved**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
You do not understand the exposure of your essential service to publicly-known vulnerabilities. You do not mitigate externally-exposed vulnerabilities promptly. There are no means to check data or software imports for malware. 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 not suitably mitigated systems or software that is no longer supported. These systems may still be running, but not in operational use.	You maintain a current understanding of the exposure of your essential service to publicly-known vulnerabilities. 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 (eg by patching) promptly. Some vulnerabilities that are not externally exposed have temporary mitigations for an extended period. You have temporary mitigations for unsupported systems and software while pursuing migration to supported technology. You regularly test to fully understand the vulnerabilities of the networks and information systems that support your essential service.	You maintain a current understanding of the exposure of your essential service to publicly-known vulnerabilities. Announced vulnerabilities for all software packages, network equipment and operating systems used to support your essential service are tracked, prioritised and mitigated (eg by patching) promptly. 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 maximise the use of supported software, firmware and hardware in your networks and information systems supporting your essential service.	• Real-time inventory of every IP-addressable device on the network and, through orchestration using Forescout Extended Modules, can compare what has been scanned by vulnerability tools and initiate a scan for any missed devices or those that joined the network between scans. • Visibility into endpoints on the network, including applications and services running on these endpoints as well as servers which can be synced in real time with the CMDB or asset record database. • Visibility into network, infrastructure and endpoint configuration controls to help ensure complete compliance.

B5 Resilient Networks and Systems			
Principle	You are prepared to restore your essential service following disruption.		
B5.a Resilience preparation			
Not Achieved	**Partially Achieved**	**Achieved**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
You have limited understanding of all the elements that are required to deliver the essential service. You have not completed business continuity and/or disaster recovery plans for your essential service's networks, information systems and their dependencies. You have not fully assessed the practical implementation of these plans.	You know all networks, information systems and underlying technologies that are necessary to deliver the essential service and understand their interdependencies. You know the order in which systems need to be restored to most quickly and effectively restore the essential service.	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 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.	**Not Applicable to Technical Tools like Forescout**
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**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
Operational networks and systems are not sufficiently segregated. Internet services, such as browsing and email, are accessible from essential service operational systems. You do not understand or lack plans to mitigate all resource limitations that could adversely affect your essential service.	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. Resource limitations (e.g. network bandwidth, single network paths) have been identified but not fully mitigated.	Your essential service's operational systems are segregated from other business and external systems by appropriate technical and physical means, e.g. separate network and system infrastructure with independent user administration. Internet services are not accessible from operational systems. You have identified and mitigated all resource limitations, i.e. bandwidth limitations.	**Forescout's CounterACT enables automated segmentation of network access by user, device classification and/or posture, regardless of how that device is connecting to the network wired, wireless or VPN. Network segregation strategies can be deployed centrally through the Forescout platform.**

B5.b Design resilience (continued)			
Not Achieved	**Partially Achieved**	**Achieved**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
		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 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**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
Backup coverage is incomplete in coverage and would be inadequate to restore your essential service. Backups are not frequent enough for your essential service to be restored within a suitable timeframe.	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. You routinely test backups to ensure that the backup process functions correctly and the backups are usable.	Your comprehensive, automatic and tested technical and procedural backups are secured at centrally accessible or secondary sites to recover from an extreme event. 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.	**Not Applicable to Technical Tools like Forescout**

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**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
People in your organisation don't understand what they contribute to the cyber security of the essential service. People in your organisation don't know how to raise a concern about cyber security. People believe that reporting issues may get them into trouble. 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 executive management understand and widely communicate the importance of a positive cyber security culture. Positive attitudes, behaviours and expectations are described for your organisation. All people in your organisation understand the contribution they make to the essential service's cyber security. 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.	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 are positively recognised for bringing cyber security incidents and issues to light, not reprimanded or ignored. 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 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.	**Not Applicable to Technical Tools like Forescout**

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**	**How Forescout can help**
At least one statement is true	All statements are true	All 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. Cyber security training is only offered to specific roles in your organisation. Records of role-specific cyber security training do not exist, or are incomplete. There are incomplete or no records of cyber security training for your organisation.	You have defined appropriate cyber security training and awareness activities for all roles in your organisation, from executives to the most junior roles. You use a range of teaching and communication techniques for cyber security training and awareness to reach the widest audience effectively. Cyber security information is easily available.	All people in your organisation, from executives to the most junior roles, follow appropriate cyber security training paths. You track individuals' cyber security training and ensure that refresh update training is completed at suitable intervals. 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. Cyber security information and good practice guidance is easily and widely available. You know this is referenced and employed by people in your organisation.	**Not Applicable to Technical Tools like Forescout**

Cyber Assessment Framework Objective C

C1 Security Monitoring			
Description	Capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential services.		
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**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
You are not collecting data relating to the security and operation of your essential services. 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 not able to audit the activities of users in relation to your essential service. You are not able to capture any traffic crossing your network boundary (e.g. even IP connections).	Network data is collected for some areas of the essential service. 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. Some user monitoring is done, but not covering a comprehensive range of user activities that might affect them. You are able to monitor traffic crossing your network boundary (including IP address connections as a minimum).	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. Your monitoring data provides sufficient detail to reliably detect security incidents that could affect your essential service. You have timely access to the data you need to use with IoCs. 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.	**Forescout Extended Modules for SIEM enable bi-directional integration with leading SIEM systems. Extended Modules for SIEM combine Forescout's device visibility, access control and automated response capabilities with the powerful correlation, analysis and search features of SIEM solutions. The result is enhanced threat insight, analytics-driven decisions and greater operational efficiency. With Forescout and popular SIEM solutions, security teams can:** • **Store Forescout device visibility data in SIEM solutions for long-term trend analysis, visualization and incident investigation.** • **Correlate high-value endpoint context from the Forescout platform with other data sources to identify and prioritize incidents.** • **Initiate Forescout control via network and host actions from a SIEM to automate incident response, remediation and threat mitigation.**

C1.a Monitoring coverage (continued)			
Not Achieved	**Partially Achieved**	**Achieved**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
			• **Demonstrate what data is accessed, by whom, how it is used and when it is deleted.** • **Forescout and Splunk customers can leverage the joint solution and Adaptive Response framework within Splunk ES for closed-loop remediation and threat mitigation.**

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**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
It is possible for logging data to be edited or deleted. There is no controlled list of who can view and query logging information. There is no monitoring of the access to logging data. There is no policy for accessing logging data. Logging is not synchronised, using an accurate time source.	Only certain staff can view logging data for investigations. Privileged users can view logging information. Some monitoring of access to logging data. Some logging datasets are synchronised.	The integrity of logging data is protected or any modification is detected and attributed. Logging data is segregated from the rest of the network, so disruption or corruption to network data does not affect the logging data. Any alterations to logging data (e.g. re-normalising for SIEM analysis) is done on copies, not the master. Logging datasets are synchronised, using a common time source, so separate datasets can be correlated in different ways. 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.	**The Forescout platform identifies users attempting to access** **logging data they are not authorized access to by their Active** **Directory group. It provides device- and role-based network** **authentication and authorization, allowing individuals and their devices to get their identified network access determined by VLANs or ACLs.**

C1.b Securing logs (continued)			
Not Achieved	**Partially Achieved**	**Achieved**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
		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**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
You are not able to investigate alerts provided by 3rd parties e.g. an antivirus (AV) provider. Your logging data is stove-piped, stored in different places and difficult to aggregate to investigate alerts. You are not able to use log data to resolve alerts to a network asset or system. You are not able to flag security alerts that relate to essential services. Logs are not reviewed regularly.	You are able to investigate AV alerts. Some logging datasets are stored centrally and can be used for some investigations. You are able to use log data to resolve alerts to a network asset or system. You are able to flag alerts that relate to your essential services. Logs are reviewed at regular intervals.	You are able to investigate AV alerts. 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 able to resolve alerts to network assets, using knowledge of the network and systems. You are able to flag alerts that relate to essential services and use this information to support your incident management capability. 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.	**Forescout can integrate with third-party advanced threat detection (ATD) and SIEM systems to provide actionable threat information that the policy manager can use to isolate or initiate remediation actions. Forescout extends the reach of existing IDS and IPS systems through Forescout Extended Modules.** • **The IDS/IPS system detects an intrusion and notifies Forescout.** • **Forescout takes network or endpoint remediation actions, such as quarantining or performing an endpoint antivirus scan.**

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**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
Your organisation has no sources of threat intelligence. You do not apply intelligence updates (e.g. AV signature updates, other threat signatures or IoCs) in a timely way, after receiving them. You do not receive signature updates for all protective technologies (such as AV and IDS) or other software in use. You do not evaluate the usefulness of your threat intelligence or share feedback with providers or other users.	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 apply some updates, signatures and IoCs in a timely way. You receive signature updates for all your protective technologies (e.g. AV, IDS). You are cognisant of how effective your threat intelligence is (e.g. by tracking how threat intelligence helps you identify security problems).	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 are able to apply new signatures and IoCs within a reasonable (risk-based) time of receiving them. You receive signature updates for all your protective technologies (e.g. AV, IDS). 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).	**The Forescout platform can help to prevent the exploitation of system vulnerabilities by:** • **Detecting hosts without an installed antivirus application, one with no running antivirus or threat signatures that are not current.** • **Denying or quarantining endpoints without installed or functional antivirus and requiring the endpoint be remediated before granting network access.**

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	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
There are no staff who perform a monitoring function. Monitoring staff do not have the correct specialist skills. Monitoring staff are not capable of reporting against governance requirements.	Monitoring staff have some investigative skills and a basic understanding of the data they need to work with. Monitoring staff can report to other parts of the organisation (e.g. security directors, resilience managers).	You have monitoring staff, who are responsible for investigating and reporting monitoring alerts. Monitoring staff have roles and skills that covers all parts of the monitoring/investigation workflow.	**Not Applicable to Technical Tools like Forescout**

C1.e Monitoring tools and skills (continued)

Not Achieved	Partially Achieved	Achieved	How Forescout can help
At least one statement is true	All statements are true	All statements are true	
Monitoring staff lack the skills to successfully perform any part of the defined workflow. Monitoring tools are only able to make use of a fraction of logging data being collected. Monitoring tools cannot be configured to make use of new logging streams, as they come online. 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 capable of following most of the required workflows. Your monitoring tools can make use of logging that would capture most common attack types. Your monitoring tools can work with most logging data, with some configuration. Monitoring staff are aware of some essential services and can manage alerts relating to them.	Monitoring staff have workflows that address all governance reporting requirements, internal and external. 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. With some configuration, your monitoring tools are able to make use of all logging data collected. Monitoring staff and tools are able to drive and shape new log data collection and can make wide use of it. 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 standard signature based security prevent/detect solutions, or when it is not possible to use signature based detection, for some reason.	
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**	**How Forescout can help**
At least one statement 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 no established understanding of what abnormalities to look for that might signify malicious activities.	You have a sufficient understanding of normal system activity (eg. 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 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.	**The Forescout platform can help restrict communications between shared information sources to ensure that only approved devices and users are accessing the data residing on the shared source (such as a SharePoint server). This is a first step in ensuring that information control is in place, by controlling who and what has access to it.**
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**	**How Forescout can help**
At least one statement is true	All 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.	**Not Applicable to Technical Tools like Forescout**

Cyber Assessment Framework Objective D

D1 Response and Recovery Planning			
Description	Capabilities to minimise the impact of a cyber security incident on the delivery of essential services including, the restoration of those services, where necessary.		
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**	**How Forescout can help**
At least one statement is true	All statements are true	All statements are true	
Your incident response plan is not documented. Your incident response plan does not include your organisation's identified essential service. Your incident response plan is not well understood by relevant staff.	Your response plan covers your essential services. Your response plan comprehensively covers scenarios that are focused on likely impacts of known and well-understood attacks only. Your response plan is understood by all staff who are involved with your organisation's response function. Your response plan is documented and shared with all relevant stakeholders.	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 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 documented and integrated with wider organisational business and supply chain response plans. Your incident response plan is communicated and understood by the business areas involved with the supply or maintenance of your essential services.	**Not Applicable to Technical Tools like Forescout**

D1.b Response and recovery capabilities	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**	**How Forescout can help**
At least one statement is true	All statements are true	
Inadequate arrangements have been made to make the right resources available to implement your response plan. Your response team members are not equipped to take good response decisions and put them into effect. Inadequate back-up mechanisms exist to allow the continued delivery of your essential service during an incident.	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. 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. 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 (eg. specialist providers of cyber incident response capability).	**Not Applicable to Technical Tools like Forescout**

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**	**How Forescout can help**
At least one statement is true	All statements are true	
Exercises test only a discrete part of the process (e.g. that backups are working), but do not consider all areas. Incident response exercises are not routinely carried out, or are carried out in an ad-hoc way. Outputs from exercises are not fed into the organisation's lessons learned process. Exercises do not test all parts of the response cycle.	Exercise scenarios are based on incidents experienced by your and other organisations, or are composed using experience or threat intelligence. Exercise scenarios are documented, regularly reviewed, and validated. 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 test all parts of your response cycle relating to particular services or scenarios (e.g. restoration of normal service levels).	**Not Applicable to Technical Tools like Forescout**

D2 Lessons Learned		
Principle	When an incident occurs, steps are taken to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents.	
D2.a Indicent root cause analysis	Your organisation identifies the root causes of incidents you experience, wherever possible.	
Not Achieved	**Achieved**	**How Forescout can help**
At least one statement is true	All statements are true	
You are not usually able to resolve incidents to a root cause. You do not have a formal process for investigating causes.	Root cause analysis is conducted routinely as a key part of your lessons learned activities following an incident . 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.	**Not Applicable to Technical Tools like Forescout**
D2.b Using incidents to drive improvements	Your organisation uses lessons learned from incidents to improve your security measures.	
Not Achieved	**Achieved**	**How Forescout can help**
At least one statement is true	All statements are true	
Following incidents, lessons learned are not captured or are limited in scope. Improvements arising from lessons learned following an incident are not implemented or not given sufficient organisational priority.	You have a documented incident review process/ policy which ensures that lessons learned from each incident are identified, captured, and acted upon. 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.	**Not Applicable to Technical Tools like Forescout**

Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591