CPNI
Centre for the Protection of National Infrastructure

CAPSS Guidance

PUBLISH DATE: July 2020

CLASSIFICATION: Official

CAPSS Guidance

v1.0, 01 July 2020

Contents

Physical Security

Executive Summary

The increasing threat

Using increasingly more sophisticated IT systems and networks to support physical security enables increased functionality and more effective surveillance. But it also introduces additional opportunities for attack, potentially by remote attackers who are similarly becoming more sophisticated.

Physical security systems now encompass an IT environment that processes, stores and transmits data relating to physical security and controls. While an organisation's existing physical security team may be very familiar with the controls being employed (such as door access control, CCTV, intrusion detection etc.) they are less likely to be familiar with the implications of using advanced IT systems to deliver and manage those controls, let alone any controls that are required in the IT systems themselves. Conversely, an organisation's IT security team should be familiar with securing IT systems, but may be less familiar with the specifics of systems that support physical security – and in most cases the physical security system will be, deliberately, distinct from other networks and systems within the organisation and therefore unable to take advantage of many of the security measures that are routinely implemented by the IT security team.

Whereas an attempt to breach traditional physical security measures tends to be localised (i.e. a specific camera, or door, or other ingress point) an attack against an IT system supporting physical security can have a more widespread impact and may affect an area that is physically remote from the attacker. An attack that targets the underlying IT may be as simple as disruption of security monitoring by disabling the network, or it may be as sophisticated as targeted malware that can take control of door opening, reposition cameras, or disable sensors.

Physical security teams must become familiar with the threats introduced by the use of IT and networks, and the controls that are required to mitigate those threats. In this document we present a series of recommended activities for organisations operating or establishing a physical security system; along with a set of detailed controls that need to be implemented to protect against the identified threats; and suggested questions to ask vendors/suppliers to determine how well their products meet the requirements of those controls.


Achieving secure Physical Security Systems
1. Identify a senior risk owner
at board level who can help and support the process.
2. Ensure that physical security and IT security teams collaborate
to define the demands of the PSS environment and achieve a workable secure solution.
3. Request that developers demonstrate compliance with CAPSS
when inviting tenders for the supply of equipment and systems. This should include evidence of a publicly stated vulnerability disclosure policy.
4. Identify the systems and environment
into which you have the physical security installed, and ensure they are suitably audited and documented.
5. Assess the risks
that are inherent in your PSS environment and identify whether further action is needed to deal with issues identified in step 4.
6. Assess the systems and environments using the NCSC CAF.
The 14 principles are written in terms of outcomes, i.e. specification of what needs to be achieved rather than a checklist of what needs to be done.
7. Identify the locations
in which your systems and devices are deployed, as defined in this document (i.e. non-secure area, secure area, secure enclave).
8. Identify where gaps exist
between the controls identified in this document and the environment you are operating.
9. Devise and implement a plan
to close gaps to ensure long-term management of any risks associated with the system. Repeat this in line with security best practice.
10. On-going monitoring
Include the Physical Security Systems within the scope of your Information Assurance processes and systems, and ensure they are continually monitored.

Introduction

In IT security an attacker may never be seen: an attack is effectively a series of signals passing down wires in an attempt to bypass the security of a system. The attacker may not need to be at the site under attack and it is often not possible to identify the individual or to prevent them from attempting their attack again. It is therefore imperative that good defences are always maintained, and detection and containment system work well to slow an attacker.

Organisations face many challenges when seeking to secure the IT components of their physical security systems (PSS). These include:

Business buy-in – Changing threat environments and increasing risk levels can be difficult to explain. If existing physical security systems have not (yet) been breached there is little buy-in for change.

Supplier service level – Interoperability of equipment is a challenge. It is difficult to switch supplier based on IT security requirements not being met or when responses to reported security issues are inadequate. This is compounded if IT security requirements are not written into the contract.

System complexity –There is little incentive to redesign systems when extensions to the requirement are identified. Modifications and enhancements to the PSS environment can result in highly complex systems that are very different from those designed from new.

System evolution – When systems are upgraded and extended the threat model should be updated otherwise new and evolving threats might not be addressed. This can lead to exposure to risk through issues inherent to legacy technologies and system architectures.

Legacy deployments – Although IT systems and components within physical security systems met operational requirements when originally deployed and have not needed to be upgraded or enhanced from a functional point of view, they are often out of date, for example in terms of protocols used and security mechanisms employed.

Separation of security teams – Physical security systems have traditionally existed beyond the IT domain. IT support for physical security systems has typically been provided by equipment suppliers without a direct connection to risk owners. The implications of this are a reduction of security and shared solutions between IT and physical security domains.

Cost of segregation – The trend in IT has been convergence towards a single network for all business services. Any argument for convergence of physical security systems with the main business network revolves around cost and security. Using a single network is often cheaper but a segregated PSS network can be more secure.

Eleven case studies are included throughout this document to illustrate the risks of not addressing the identified threats.

The decision-making framework in this document enables an organisation to understand the threats that need to be addressed and the risks inherent in leaving them unaddressed, as well as enabling the organisation to work out (for their specific environment) what their own priorities should be if they don't have the option to use CAPSS compliant products.

Current landscape

Physical Security System environment

In most cases, a Physical Security System will consist of a number of different products addressing various aspects of a protection objective, where each product may have been provided by one or more suppliers from one or more developers. There are three types of location wherein an element of the system can be deployed:

Non-secure area – an area that is not secured, such as public spaces and building exteriors. This would also include areas such as shared office building reception that may be 'supervised' but are not controlled.

Secure area – a secured area with access limited to authorised personnel and escorted unauthorised personnel and visitors (some of whom may be unescorted for periods of time). This would be likely to include controlled offices but not meeting rooms (especially if external personnel have access to the room).

Secure enclave – a secured area with access limited to a deliberately minimised list of individually authorised personnel, no unescorted access for unauthorised personnel, visitors only if escorted, and records of access. Typically, a secure server room or secure control room. See [CPNI CtrlRms] for guidance.

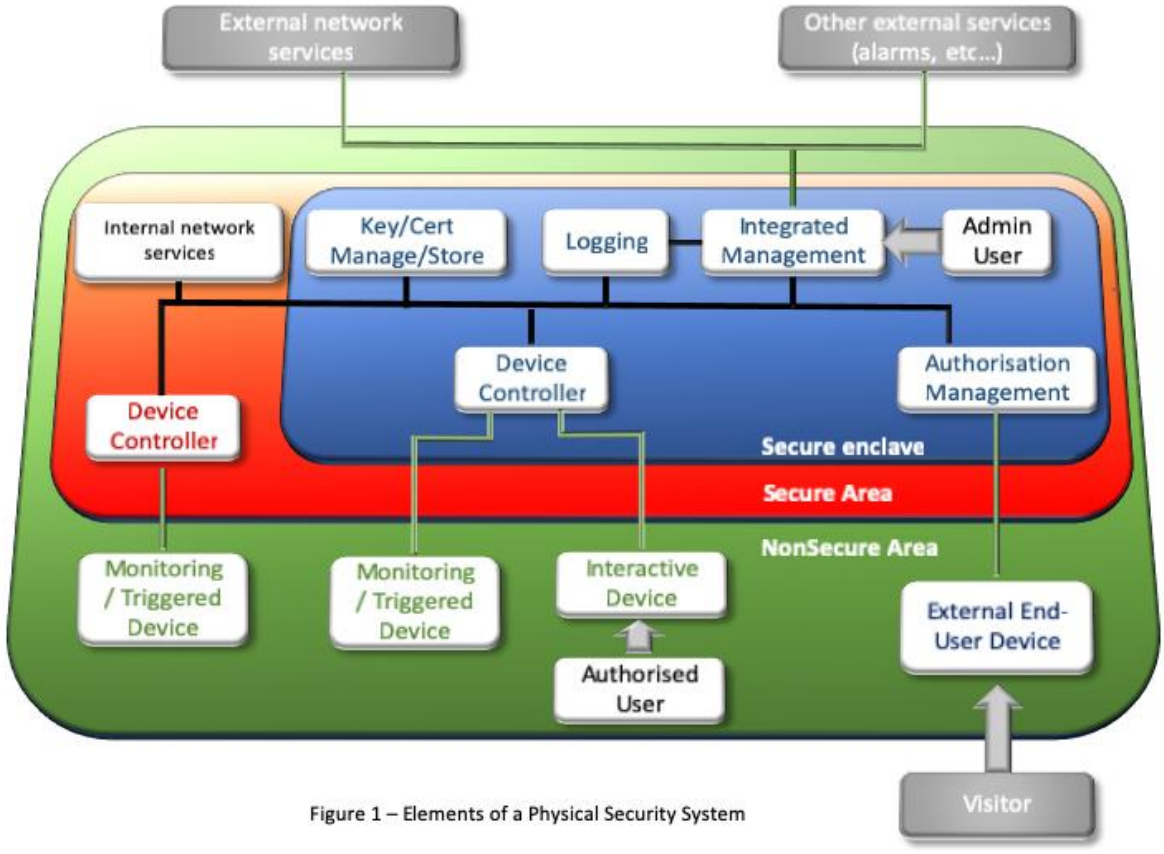


Figure 1 – Elements of a Physical Security System

Figure 1 above illustrates the types of element that are likely to be included in such a system. Some elements will necessarily be deployed in exterior, public or otherwise non-secure areas, and will generally be unattended once deployed. Other elements such as controllers and management systems must be deployed in one or more secure areas. Some must be deployed in a secure enclave, typically servers and other storage devices but also management access for those elements. External services may be required, including provision of network connectivity, reliable time services, or for sending alarms to other organisations such as emergency services. Typically, subsets of products will be installed as a subsystem consisting of elements in both secure and non-secure areas, requiring communications between them. Such subsystems may operate independently or integrated with other subsystems.

(For an example of the importance of defining security requirements relating to the PSS environment, see **Case Study – System requirements** below.)

Figure 2 shows a typical implementation, where a Command & Control subsystem implements the Integrated Management, Logging and Admin functions; an AACS subsystem is an example of a controller with a deployment of interactive devices to permit access for authorised users; a CCTV subsystem is used for monitoring; a physical intrusion detection system deploys movement and infra-red sensors; a perimeter monitoring system deploys exterior sensors; and a Visitor Management system manages access by visitors with a reception workstation.

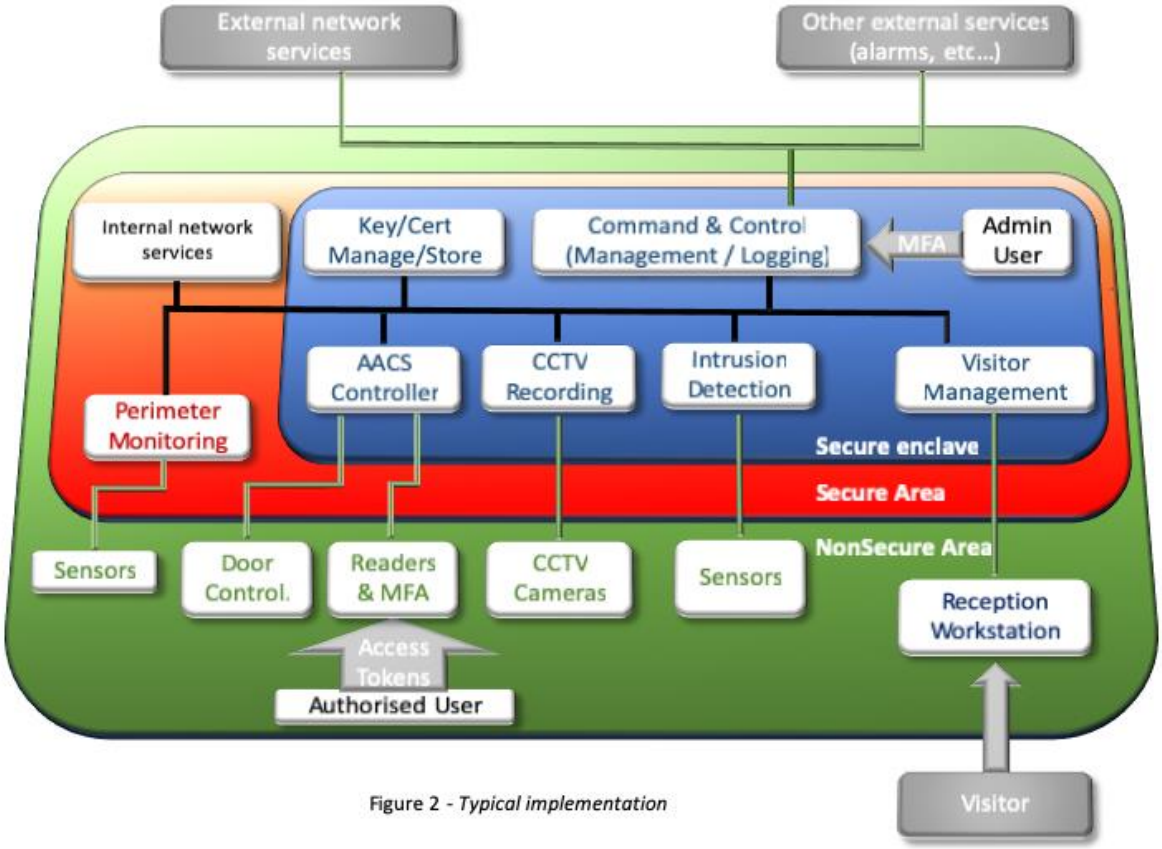


Figure 2 - *Typical implementation*

The variety of systems, subsystems and discrete elements of which a physical security system may be comprised, means that for each element different threats may be applicable leading to risks which are determined by architecture and communications. In particular, risks will vary for elements depending on whether they are intended to be deployed in a non-secure area, secure area, or secure enclave. At a specific site there may be elements deployed in a secure area that are also intended to be suitable for deployment in a non-secure area (such as CCTV or sensors) – in this case the requirements for non-secure area deployment should still be applied. However, devices that are intended to be deployed in a secure area must not be deployed in a non-secure area. CPNI has established the CPNI Cyber Assurance of Physical Security Systems (CAPSS) standard [CPNI CAPSS] for products to be used in a PSS environment. Elements are categorised within the CAPSS standard as follows:

- **Secure enclave device** – this encompasses all devices, subsystems or systems that are entirely deployed within the perimeter of the secure enclave; these are assumed to be highly functional devices (e.g. in a secured server room).

- **Secure area device** – this encompasses all devices, subsystems or systems that are deployed within a secure area but outside the secure enclave; these devices are assumed to be highly functional devices (e.g. in an area with restricted access).

- **Non-secure area device** – this encompasses devices within the non-secure area. This includes devices that are deployed to interact with users and are therefore accessible by potential attackers and might not be overseen (for example, access control token readers and keypads); and devices that are deployed to monitor or act as sensors, do not require direct user interaction and, although they might not be overseen, are intended to be deployed out of easy reach of potential attackers (for example, CCTV cameras, motion detectors, door opening sensors).

- **External end-user device** – this encompasses devices in the non-secure area that enable interaction with a system inside the secure area (for example, visitor registration workstation or tablet) but that are likely to be overseen.

It is anticipated that products will be implemented on a wide variety of platforms, ranging from software products deployed on a standard PC or server, to small embedded systems in sensor devices. This needs to be taken into account when identifying the general applicability of controls and may require further consideration for particular implementations.

Associated infrastructure

A number of additional devices and systems, over and above what is shown in Figure 1 and Figure 2, are needed to deploy a physical security system over an IP network. The key components are:

Switches: devices to connect different Ethernet ports together and allow traffic to flow from one device to another. Switches can offer the capability to enforce rules on what communications are allowed or which devices can connect. However, switches are often delivered in an insecure configuration and it is important that some basic precautions are taken during installation to protect them from attack (e.g. changing any default passwords). This will often be highly product specific, and the developer should provide guidance on how to secure their devices.

Routers: devices that connect different networks together, typically allowing IP traffic to route from one network to another. As with switches, routers can enforce rules on communications. Depending on the developer of the router there is also typically a best practice approach to configuration. Poorly configured routers may lead to compromise of traffic through the router. For further guidance see [NCSC Router].

Firewalls: devices that can be placed between connections and are typically configured to block all connections except those explicitly allowed. They are an important control that prevents network devices from communicating with each other in ways other than those that have been defined. In some cases, firewalls will be separate devices, however the functionality can be included in routers or switches or in the end-user systems themselves. Firewalls can be used to control any traffic between a PSS network and an organisation's corporate network, in particular to ensure that unauthorised traffic from the corporate network cannot enter the PSS network whilst at the same time allowing traffic from the PSS network to communicate with devices on the corporate network as required (such as a domain controller or email server). For guidance see reference [NIST Firewalls].

Anti-malware/anti-virus server software: aims to detect viruses and other malware but is dependent on regular, sometimes daily, updates to inform it of current viruses. As such, enterprises will often have a server which communicates with anti-malware software running on desktops to obtain updates. In corporate networks the central server typically connects to the developer's system across the internet to obtain these updates; however, in a PSS environment a manual process may be required if internet connectivity is not directly available.

Security patch and update server: Security patches are usually obtained directly from the operating system or software developer. However, enterprises will often use a centralised patch distribution server as it allows the enterprise to manage the deployment across the estate. The technology used will determine whether it is possible to distribute updates for both the core operating system and additional software applications through this mechanism. In a PSS environment the main consideration for the use of such a system is whether a manual patching process can be supported given the scale of the environment. See reference [NIST Patch] for information about software patching solutions. A comprehensive Update Policy (see below) is the most effective way to ensure that updates for any and every component in the environment are managed appropriately.

Domain controller: Windows systems can join a domain whereby users and policy can be managed centrally rather than requiring administration of individual workstations. A domain controller is a server that manages authentication and authorisation of users and the policies that are applied to systems in the environment. The current mechanism for storing and accessing user and policy information is called Active Directory (AD) and can be used to create logical containers for users, systems, groups and roles within the environment. AD is a powerful tool capable of supporting vast estates although it is equally adept with small, self-contained systems. In a PSS environment containing a number of Microsoft Windows workstations and/or servers, Active Directory and a domain controller can be very useful for managing security, although it is not trivial to apply effective design and configuration to ensure that the domain controller itself cannot be compromised and used to launch attacks against those systems administered through it. See reference [MS SecuringAD].

Application servers: In PSS environments it is common for components of the system to run on servers which are installed with a specific software application, e.g. an intrusion detection system will use an application server to query the sensors and to display the results to the operators. This is achieved by running services on the system that can be accessed across the IP network. The software used in these environments is primarily proprietary to the physical security equipment developer and often will not use open standards or protocols for communication. Secure setup and configuration of the software component will be developer- and product-specific; in addition, the underlying operating system can be subject to secure configuration. See references [NIST Server], [NIST Telework] and [NCSC Servers].

Workstations: In a PSS environment alarm data and camera feeds are displayed on screens in the control room to enable security personnel to identify and respond to intrusion attempts and security exceptions. If analogue systems are used these pictures are driven directly from the cameras. When communication over IP is used these pictures are typically displayed from a PC workstation. This system will often run product-specific software that communicates with application servers and shows the status of a camera or sensor alerts on screen. As with application servers these systems should be subject to secure build and configuration. See references [NIST Telework], [NCSC Mob] and [NCSC Servers].

Support laptops: Once a PSS system is installed and configured, it is necessary to perform administrative tasks from time to time to ensure safe and reliable operation of the system. This can require dedicated laptops, as it may be necessary to connect directly to components using developer-specific software. However, if not correctly secured, configured and maintained, the laptops may introduce risk if, for example, they have malware that subsequently spreads to systems in the environment or if they do not implement sufficiently strong authentication. See reference [NCSC Mob].

Event logging system: Events such as failed or successful logins are typically logged by the system on which the event occurred. However, it can be useful to aggregate the logs on a central logging server to permit easy analysis and alerting. Individual computers will upload their logs to a central server, which can then manage alerting or monitoring. Administrative or security staff should be able to access the central logging host and thereby easily review the logs for all servers at once. It is often desirable to consolidate all alerting across an organisation into a centralised system although this does not typically occur when the PSS environment is separate from the corporate IT environment. For a guide to log management see reference [NIST Log], [NCSC Log].

Necessary Policies

In order to deploy and manage the complex variety of devices, systems and infrastructure, it is essential to have well defined policies and processes to ensure correctness, consistency and completeness. This also helps to avoid critical information being lost or unavailable because of a dependency on a single individual (see **Case Study – The undocumented network** below).

The key policies are detailed over the next few pages:

Maintenance Policy (including Update Policy): A policy that deals with how maintenance is to be carried out on the system and its components. One important part of this policy is an Update Policy that identifies how, when and why updates are applied to the devices, systems and products in the PSS environment. For each of these components of the environment, the update policy needs to address the process(es) by which updates are notified, how updates are delivered, how they are authenticated and authorised, how they are applied and (where appropriate) how they are tested before being rolled out to the live PSS environment. If updates are to be applied to multiple devices, the update policy needs to include how to ensure that the updates are compatible and whether they need to be rolled-out simultaneously or in a specific order. The update policy should also address what to do when components (hardware or software) are no longer supported, reflecting the need to avoid situations where hardware spares may become difficult to obtain, or software updates may no longer be available to patch discovered vulnerabilities (cf. **Case Study – The cameras that went dark** below). For guidance on dealing with software obsolescence, see [NCSC Obs].

Other aspects to address in the Maintenance Policy include: requirements for routine maintenance access and access in response to failures (this may include both logical and physical access), requirements for swapping hardware components (including whether or not devices are allowed to be removed from the site), requirements for reprovisioning, and requirements for end-of-life for system components (e.g. sanitisation of sensitive date before disposal). Guidance on both reprovisioning and end-of-life are addressed in the [NCSC Reprov] EUD guidance on 'Factory reset and reprovisioning' and in [NCSC Mob] under 'Erasing mobile devices' as part of the 'Managing deployed devices' section. See **Case Study – A single point of failure** and **Case Study – System requirements** below, and **Case Study – No test environment** later in this section, for examples of problems that this policy should prevent.

Case Study – The undocumented network

Whether conducting an audit of security within a physical security environment or responding to an incident it is essential that representative and up-to-date documentation is available. Without this information the task of identifying security weaknesses is difficult and incident response is more costly and more disruptive to the business. In one organisation, the design and construction of the network supporting the physical security system only existed inside the head of one key employee, rather than in system documentation and diagrams. The individual's management chain did not understand the importance of documenting the system and therefore did not pursue it as a key objective. When there was an incident affecting the CCTV cameras it was not possible to respond to it until this individual was available to assist. Additionally, it was not possible for the specialists called in to conduct the investigation to make progress until the system architecture had been documented. The lack of documentation added at least two working days to the start of the investigation. As a result, the site was without CCTV coverage for an extended period until the source of the problem had been identified and the affected component had been identified and replaced. **It is essential that the system architecture is documented and kept up-to-date and does not rely on the availability of specific members of staff.**

Case Study – The cameras that went dark

If it ain't broke, don't fix it – is not an appropriate policy for a security system.

Compared with other IT systems in an organisation, the physical security systems often suffer from this approach – even when the equipment developer goes out of business the systems aren't upgraded. As a result, systems lack developer support and spare parts and there is an inability to deploy new devices within the environment.

In one company, the CCTV system operated without major incident for five years after the original developer had gone bust. During this time spares and new devices became increasingly scarce until eventually they could only be acquired through online auction sites. When key components of the CCTV environment then suffered hardware failures it was not possible to restore the service until a completely new system had been designed, sourced, procured and installed. This process took over six months to complete and during that time the site was effectively operating blind and relying solely on manned guarding to provide physical security (the cost of extra guarding being many times more than the cost of the entire new CCTV system). These costs would have been avoided if the upgrade project had been instigated in the time between the developer going bust and the system failure occurring.

This highlights why the availability of maintenance and support for all developer equipment on the physical security system is significant and why upgrades are sometimes necessary even if the system is apparently functioning correctly.

Case Study – A single point of failure

Maintenance contracts and service level agreements should cover all the key components of the Physical Security system. Whether it's replacing a faulty camera or repairing a door controller, they all fall under the terms of the support contract. Additionally, as it's unlikely that more than one camera or sensor will fail at one time the scenario of a component failure will often be built into a site's Operating Procedure. One thing often forgotten is the network infrastructure that supports these systems. What happens if the network switch that feeds all the terminals and monitors in the control room fails?

In one organisation, there was a control room that acted as a central hub for all physical security monitoring activity within the facility. All the systems that fed into this control room used a single Ethernet switch to carry the communications between the main network and the PCs that displayed images on the screens. When this network switch suffered a hardware failure it effectively blacked out the control room and prevented access to all live CCTV images and intrusion detection system alerts. The network switches were not covered by the support arrangements, so it took several days to source a replacement device through the authorised procurement channels. To complicate matters further the configuration details had not been backed up and further delays were experienced. During this time the control room was out of action.

It is important to identify single points of failure in the network supporting physical security systems and ensure that appropriate mitigations are put in place for maintenance, replacement and restoration of configuration. Having a well-documented and mapped system will assist with this.

Case Study – System requirements

When outsourcing any aspect of IT, it is important that the scope and terms of the agreement are aligned with the ongoing needs of the organisation to avoid ad-hoc change requests that incur additional costs. This is certainly a consideration when the maintenance and management of a physical security system is outsourced to a 3rd party supplier. A failure to specify adequate security-related activities in the initial contract can leave the system exposed to attack or can result in significant additional costs. Typically, the physical security requirements are mapped to a set of IT system requirements; however, the security of the IT system itself is often not included within the scope.

One organisation's contractual agreement with a 3rd party supplier included no wording or reference to maintaining the security of the IT systems that supported the physical security controls. After an audit of the PSS environment was conducted, a number of additional management processes were recommended including the installation and updating of anti-malware software, the installation of software security patches, auditing of user accounts and monitoring of log files. However, the cost of the 3rd party completing these processes (which were outside the contractual agreement) was calculated to be too high to fit within the constraints of the physical security budget and the processes could not be implemented internally as the organisation's IT function would not support the 3rd party's software build. This situation was compounded by the fact that the 3rd party would not continue support of the software components if the internal IT function adapted the Operating System. As a result of a long term contractual lock-in the issues could not be resolved and the close relationship between the 3rd party and the physical security team prevented the issue being escalated internally. If the organisation had mapped out their IT security requirements during the initial contract negotiations this issue would have been avoided.

It is important to ensure that security requirements of the PSS environment and systems are well-defined and included in the requirements of any agreement, whether it is with an internal IT or security department or an external 3rd party supplier or service provider.

Backup Policy: A policy that identifies how, when and why backups are made of configurations, security settings, data, logs and any other data that is essential to the operations of the PSS environment. The policy needs to identify the types of data that require backup and any relevant characteristics that affect the necessary backup regularity or approach for that data (for example configuration settings that remain unchanged in use only need to be backed up after configuration; while log data may need to be backed up on a regular or even continuous basis). It needs to identify the process(es) to be used to ensure that backups are securely performed and can be reliably restored in a timely fashion in the event of a failure or to recover from a compromise (for example by testing regularly that backups can be restored). It is not unusual for separate backup regimes to be required for separate devices, in particular where some products include their own backup features.

Leavers Policy: A policy that defines what actions must be taken in the event of the departure of personnel or third parties who have been granted access to any of the PSS environment. The policy needs to ensure both that necessary access is maintained by transferring to another person, and that the leaver's access permissions are removed in a timely fashion, whether that is managed locally within the PSS environment or at an organisational level (such as accounts in an organisation-wide Active Directory). It also needs to ensure that passwords to any systems (or other security information such as combination codes) that were known to the leaver are changed immediately, and that all physical access tokens or keys have been returned or disabled (see **Case Study – The forgotten user accounts** below).

Compliance: Every organisation is required to comply with Data Protection legislation. It is recommended that the organisation's legal department is consulted in defining a policy to ensure that any data captured via PSS systems is handled correctly and in compliance with applicable legislation. In particular this needs to include consideration of backup and archive data, as well as access to data used during testing or maintenance.

Testing Policy: A policy that identifies how, when and why testing is conducted. The policy needs to define the testing approach to be taken when the PSS environment is deployed or changed. This should include the criteria to determine whether tests can be applied to the live PSS environment (such as during an out-of-hours test) or if they should be applied in a separate test environment (see **Case Study – No test environment** below). This will need to be compatible with the Update Policy (see above). The testing policy also needs to address the organisation's approach to periodic testing (such as annual penetration tests).

Case Study – The forgotten user accounts

In one organisation, when an employee left or changed role their account on the operating system of their automatic access control servers was not revoked at the same time as their physical access rights, because the leaver's process did not take account of people having this type of access. As a result, the employees still had access to the automatic access control system and could therefore manipulate their privileges from within the Operating System itself. They only needed access to the company's IT network to be able to add themselves as a user with access to any part of any site controlled by this system, even though other access rights had been revoked.

This illustrates why all systems on the physical security network should be included in the leaver's process and why regular audits of all user accounts within the system should be completed.

Case Study – No test environment

One of the key components for obtaining assurance in any environment is security testing, or penetration testing. During this activity the key security controls in the system are tested to determine if they behave as expected or whether there are methods of circumventing or defeating them. This is especially true with physical security systems as the effectiveness of IT security controls can have a big influence on the overall protection of the site. However, by its very nature security testing is intrusive and aims to disrupt the operation of the systems, albeit in a controlled manner. As a result, testing can have unforeseen implications for the security of the environment.

One organisation conducted a security test but did not have a test or development environment for their physical security system. Therefore, the test had to be carried out against the live system. There were several implications – not least that testing was more costly to perform as additional safeguards needed to be built into the process. When a number of significant weaknesses were identified in the system as a result of the testing there was no way to validate fixes and configuration changes before they were applied to the production system. As a result of the challenges that were encountered during this process the organisation decided to build and run a small segregated development environment, which was a key resource during subsequent security tests and audits.

When designing a PSS environment, consider the requirements for future upgrades and tests, planning for a means to test significant updates before they are rolled out to the live systems.

Security controls

The CPNI Cyber Assurance of Physical Security Systems (CAPSS) standard [CPNI CAPSS] identifies minimum baseline requirements for physical security systems, for evaluation, certification, and inclusion in the Catalogue of Security Equipment (CSE) published by CPNI. CAPSS evaluation is not a guarantee of freedom from security vulnerabilities – there remains a probability that exploitable security vulnerabilities may exist in the product or the information systems environment supporting the product. However, the purpose of CAPSS evaluation of products is to ensure a progressive improvement of the security of products deployed in critical locations.

Ideally, therefore, an organisation specifying a new PSS installation, or upgrading an existing installation, should be able to specify and deploy products from the CSE for which the developer has obtained a CAPSS certificate. However, while developers are becoming familiar with the standard and the benefits of CAPSS certification, there are various types of products for which there are currently no evaluated products. The security controls identified in this document are derived from the requirements specified in the CAPSS standard allowing an organisation that is unable to deploy evaluated products to address the threats that the standard is intended to counter. For each control, the *Threat* is presented (identified as in the CAPSS standard, followed by a brief explanation of what it means in practice); along with information to *Ask* for from the product developer/supplier (e.g. in an Invitation to Tender) to assess whether the threat can be addressed; and *Action* to take to implement a suitable control. They are grouped together according to the type of threat that is being addressed, and identified with a reference to the CAPSS standard (mitigation number and name, e.g. “Wireless network must be secured – CAPSS Ref 401”), so that where a certified product is (subsequently) used, it will be clear how it addresses the guidance in this document. The groupings are as follows:

Network. Threats here relate to the exploitation of insecure networks or connected networks; the exploitation of unreliable/unsynchronised time; and the exploitation of insecure interfaces.

Administration. Threats here relate to the exploitation of misconfiguration or ability to alter configuration; the introduction of compromised software; and the exploitation of inadequate account/privilege management.

Physical protection. Threats here relate to tampering; interruption to power; and the exploitation of insecure interfaces. Products that are deployed in a non-secure area may have different requirements from products that are deployed in a secure area or secure enclave.

Data protection. Threats here relate to the extraction of sensitive data.

Malware protection. Threats here relate to the introduction of malware.

Product quality. Threats here relate to the exploitation of software implementation errors.

Monitoring. Threats here relate to the sanitising of evidence from logs.

Alongside the use of certified products, where available, it is recommended that all organisations, but especially critical infrastructure, should conduct an assessment using the NCSC Cyber Assessment Framework (CAF) [NCSC CAF]. This consists of an assessment against 14 principles, which are written in terms of outcomes, i.e. specification of what needs to be achieved rather than a checklist of what needs to be done. Assessment using the CAF will help to identify areas where outcomes are not being achieved and the controls identified in the current document will enable the underlying issues to be addressed.

In addition, a number of good cybersecurity design practices and developer processes are identified in [ETSI EN303645]. Although the title of this standard refers to Consumer Internet of Things, the principles are widely applicable, and it is recommended to check that these have been followed (where applicable to the system in question).

Risk Overview

The table below provides an overview of the controls that are defined in this section, mapping them against factors of complexity and cost, but especially risk. The **Complexity** column provides an indication of the relative ease or difficulty of implementing the control within an existing PSS environment – there are many factors that could influence this and therefore the ease of implementation should be reviewed in each case. The **Cost** column provides a relative cost for illustrative purposes, as it is clearly not possible to provide accurate estimates for the cost of each of the controls in any specific implementation. The **Risk** column indicates the level of risk if the identified control is not in place to mitigate the identified threat.

Risk	Complexity	Cost	Name	CAPSS Ref	Control Section
High	Low	Low	Evaluation/Cryptocheck	100	Product Quality
High	Low	Low	Encrypt sensitive data	105	Data Protection
High	Low	Low	Secure software delivery	107	Administration
High	Low	Low	Protected software environment	108	Product Quality
High	Low	Low	Unique security data per device	109	Data Protection
High	Low	Low	Disable non-operational logical and physical interfaces	200/200	Network/Physical Protection
High	Low	Low	Tamper response	201	Physical Protection
High	Low	Low	Protection of security-related physical structure	203	Physical Protection
High	Low	Low	Physical security of management interfaces	204	Physical Protection
High	Low	Low	Ensure product security configuration can only be altered by an authenticated system administrator	301	Administration
High	Low	Low	Deploy onto suitably protected endpoint	303	Malware Protection
High	Low	Low	Wireless network must be secured	401	Network
High	Low	Low	Do not deploy wireless technology at sites requiring more than a basic level of protection	408	Network
High	Low	Low	Role based access control	500	Administration
High	Low	Low	User least privilege	501	Administration
High	Low	Low	User authentication	502	Administration
High	Low	Low	One administrator per account	503	Administration
High	Med	Low	Updateable product	106	Product Quality
High	Med	Low	Remote management authentication	505	Network
High	Med	Low	Log all relevant events	600	Monitoring
High	Med	Med	Use segregated networks	404	Network

High	Med	Med	Encrypt communications traffic over untrusted link	406	Data Protection
High	Med	Med	Protocol robustness testing	407	Network
High	Med	Med	Local management authentication	504	Network
High	Med	Med	Suitable cloud services	700	Network
Med	Low	Low	Fail secure on power loss	202	Physical Protection
Med	Low	Low	Minimise interfaces	400	Network
Med	Low	Low	General resource management	405	Network
Med	Low	Low	Record when device last seen	604	Monitoring
Med	Low	Med	Audit log review	603	Product Quality
Med	Med	Low	Administrator authorised updates	110	Administration
Med	Med	Low	Use whitelist to limit communications	402	Network
Med	Med	Med	Heap hardening	101	Product Quality
Med	Med	Med	Stack protection	102	Product Quality
Med	Med	Med	Data Execution Prevention	103	Product Quality
Med	Med	Med	Address Space Layout Randomisation	104	Product Quality
Med	Med	Med	Ensure product security configuration can be backed up	302	Administration
Med	Med	Med	Use time synchronisation	403	Network
Med	Med	Med	Protect access to logs	601	Monitoring
Med	Med	Med	Export logs	602	Monitoring
Med	Med	Med	Synchronised event timestamps	605	Network
Low	Low	Low	Provide a configuration tool to enforce required settings	300	Administration

The details of all these controls are provided in the following sections.

Network

Name	Description
Disable non-operational logical interfaces **CAPSS Ref 200**	**Threat: Exploitation of insecure internal or external interfaces** *Interfaces that are not required for normal use could be used to undermine the device security, if they can be accessed by an attacker.* Interfaces that are not required for normal use need to be disabled. This includes debug interfaces within the device, and any development, testing or configuration interfaces accessible either within the device or externally. **Ask**: Ask the developer to confirm what interfaces are available in the product, how they are disabled in normal use; and that the product's deployment guidance includes any administrator action required to disable interfaces. **Action: Ensure that any measures to disable interfaces that are identified in the product's deployment guidance have been implemented.**
Minimise interfaces **CAPSS Ref 400**	**Threat: Exploitation of an operational or non-operational interface through crafted input** *If a device leaves protocols and services available that are not necessary for it to function, these not only become potential interfaces through which the device can be attacked they are also less likely to have been secured in any way by the developer.* **Ask**: Ask the developer to confirm that there are no unnecessary ports or services available on the device that are not required for it to function. Ask the developer to confirm that any administrator actions required to disable interfaces are clearly identified in the product deployment guidance. **Action: Ensure that administrators carry out any actions required to disable interfaces on the devices. Include firewalls (with rules to prevent access to any remaining unused interfaces) and a DMZ, if appropriate, between the PSS network and any other connected network (such as the organisation's existing network or an external network such as the internet) to reduce the opportunity for external attackers to attempt to exploit devices.**
Wireless network must be secured **CAPSS Ref 401**	**Threat: Exploitation of unsecured wireless network** *Wireless networks without suitable security mechanisms can be trivially intercepted and easily compromised.* Wireless technologies must not be used on any site requiring more than a basic level of protection. **Ask**: Ask the developer what wireless technologies are implemented; if WiFi is implemented, does it support WPA2 Enterprise security? **Action**: Ensure that WiFi connections use WPA2 Enterprise as a minimum. Where the use of Bluetooth or other wireless networking protocols is unavoidable, ensure the use of secure protocols at higher levels in the communications stack (such as TLS) to provide encryption and authentication protection, employing NIST-approved cryptographic algorithms.

Name	Description
Use whitelist to limit communications **CAPSS Ref 402**	**Threat: Messages from unauthorised devices** *Accepting messages from an unknown source makes a device much more susceptible to an attack.* Messages attacking a device are likely to originate from an unknown source. Products need to check the provenance of messages, by using a whitelist feature to ensure that communications are from devices that have been previously authorised. Although this can be as straightforward as MAC filtering, [IEEE802.1X] is preferred. Messages from a device not on the whitelist need to be rejected or ignored. **Ask**: Ask the developer whether the product provides a whitelist feature. **Action**: If the product provides a whitelist feature, ensure that the deployment guidance is followed to correctly configure it during installation. If there is a choice of measures, use [IEEE802.1X].
Use time synchronisation **CAPSS Ref 403**	**Threat: Exploitation of variations in time between devices** *Unsynchronised time on various devices makes it difficult to correlate activity between devices and may enable subversion or spoofing of messages between devices.* Use of a reference time source ensures time synchronisation between devices. The time source can be an external time server or an internal time server with a trusted time source, using a suitable protocol such as NTP or PTP. **Ask**: Ask the developer to confirm that, where time can be set directly on a device, this can only be performed by an authorised and authenticated administrator. **Action: Establish a reference time source and use the product deployment guidance to configure devices to use it.**
Use segregated networks **CAPSS Ref 404**	**Threat: An attack through a connected network** *Connecting to other networks introduces the risk of attacks from a compromised device on another, potentially less well-protected, network.* Segregated networks ensure that unrelated components are kept separate, reducing the opportunity for attacks from a compromised device. **Ask**: Ask the developer whether the product supports the use of segregated networks. **Action**: Ensure that the product is configured using segregated networks. As a minimum any management interface must be on a separate VLAN.

Name	Description
General resource management **CAPSS Ref 405**	**Threat: A Denial of Service attack from a network interface** *A Denial of Service attack subjects a device to unusually large amounts of traffic causing it to crash, fail, or impair its functionality.* A device needs to protect against instability when processing incoming network traffic, to ensure that large amounts of traffic do not cause the device to crash or suffer a general failure, through implementation weakness or simple resource exhaustion, resulting in loss of functionality (apart from temporarily losing external communications). **Ask**: Ask the developer to confirm the device's behaviour in the event of large amounts of incoming network traffic. **Action**: Ensure that administrators are aware of any specific action that needs to be taken to protect the device from excessive traffic, or in the event of failure of the device.
Protocol robustness testing **CAPSS Ref 407**	**Threat: Exploitation of an operational or non-operational interface through crafted input** *Interfaces between devices may only have been tested for correct response to valid messages (or for only a few variations on valid messages). Carefully crafted invalid messages can often cause incorrect behaviour of interfaces revealing information useful to attackers, or even subvert the security mechanisms employed by the interface.* Many protocols are very complex, with various record types and data formats embedded, and hence a large number of different permutations of message contents that are valid or invalid. The increasing complexity of the protocols, and the fact that testing often concentrates only on the behaviour on receipt of valid messages, means it is more likely that the software handling the protocols has flaws in the way it handles abnormal conditions. Fuzz testing has been found to be a reasonably efficient technique to test software that is required to handle complex protocols. Interfaces between components of a product and from the product to other devices need to have been tested using fuzz testing techniques to provide a reasonable level of assurance of correct behaviour when under attack. **Ask: Ask the developer for evidence that the protocol implementations on the product have been subjected to fuzz testing.**
Do not deploy wireless technology at sites requiring more than a basic level of protection **CAPSS Ref 408**	**Threat: A Denial of Service attack, identification of a device through network advertising, or a man-in-the-middle attack on device communications** *The use of wireless technology provides opportunity for network attacks without the need for direct connections.* All device communications must occur over wired network connections if deployed on a CNI site requiring more than a basic level of protection. **Ask**: Ask the developer whether the product can be deployed without the use of wireless technologies and whether, if present, they can be disabled. **Action**: If the site requires more than a basic level of protection, ensure that the product is deployed without the use of wireless technologies and that, if present, they are disabled.

Name	Description
Local management authentication **CAPSS Ref 504**	**Threat: Exploitation of poorly protected management interfaces** *Compromise of an administrator's account (whether by social engineering or the use of malware) is a common route to attack or subvert a system. Single factor authentication (such as username/password) is highly susceptible to such targeting.* The elevated privileges assigned to admin accounts makes them a more likely target for attackers, so admin accounts need to be protected by using Multi-Factor Authentication (MFA) for admin users. **Ask**: Ask the developer to confirm that an MFA authentication mechanism can be employed for admin user accounts. **Action: Enforce the use of MFA authentication that is unique to each admin user.**
Remote management authentication **CAPSS Ref 505**	**Threat: Exploitation of poorly protected management interfaces** *Remote access provides an easy route to attack a device or system.* Therefore, remote access needs to be disabled by default and require specific action during installation (or subsequently) to enable it. Remote management access needs to be protected by a secure protocol and MFA authentication. **Ask**: Ask the developer to confirm that remote access can be disabled unless it is specifically required; and that any remote management interface can be protected by a secure protocol, such as IPsec, SNMPv3, TLS or SSH with MFA authentication. Ask the developer to confirm that there are no undocumented nor unauthenticated developer-installed accounts (see **Case Study – the developers backdoor**). **Action: Ensure that remote access is disabled unless it is specifically required. Ensure that any remote management interface is protected by a secure protocol, such as IPsec, SNMPv3, TLS or SSH with MFA authentication.**
Synchronised event timestamps **CAPSS Ref 605**	**Threat: Modification of logging generation** *Unsynchronised time on various devices makes it difficult to correlate log records created by different devices and may enable modification or spoofing of log records to remove evidence of an attack.* Event timestamps need to be synchronised with a reliable time-source. **Ask**: Ask the developer whether the product ensures that time stamps in logs are synchronised between all of its component devices, so that all logs are based on the same time. **Action: Ensure that event timestamps are synchronised with a reliable time source.**

Name	Description
Suitable cloud services **CAPSS Ref 700**	**Threat: Exploitation of insecure cloud services** *Cloud services that do not implement suitable security provide increased opportunity for network attacks.* The developer of any product using external cloud services must state how they meet the NCSC Cloud Security Principles as defined in the NCSC Cloud security guidance [NCSC Cloud]. The cloud service provider must have published their response to the NCSC Cloud Security Principles. **Ask**: Ask the developer whether the product requires the use of external cloud services; if so, ask for a statement of how they meet the NCSC Cloud Security Principles. Ask for a published response by the cloud service provider to the NCSC Cloud Security Principles. **Action**: If any product uses external cloud services, ensure that guidance is obtained and followed to ensure that the configuration meets the NCSC Cloud Security guidance.

Case Study – Remote access

In general, CPNI recommends that your physical security systems are on a segregated network that does not connect to your main corporate environment. However, in this case it is important to anticipate remote access needs. In many environments the 3rd party providing support and maintenance of the systems requires access for troubleshooting.

An organisation identified that their 3rd party support company was using 4G dongles to access systems over the internet. They were also using technologies such as 'GoToMyPC' to enable the systems to be remotely accessed by their offsite support team. These methods of remote access meant that data from the network was being sent across the public internet without appropriate encryption and was passing through 3rd party systems. Both violated organisation Y's IT security polices and were not appropriately controlled, audited or monitored. This highlighted the importance of providing secure solutions to support the requirements of the environment.

In this example, support and maintenance required remote access to systems, it was therefore important to design and implement the environment to enable remote access and to identify the security controls required to ensure that it was secure and complied with the security policies.

Administration

Name	Description
Secure software delivery **CAPSS Ref 107**	**Threat: Installing compromised software** *Attackers may spoof software sources to deliver compromised software which provides them with access or control or disrupts a device's operation.* The authenticity of software is essential to ensure that compromised software is not installed in a product. Cryptographic mechanisms need to be used to assure the integrity and authenticity of the software, both for initial installation and subsequent software updates. Most software should acknowledge the possibility of vulnerabilities being discovered in future and should therefore provide a secure update method. However, in some cases, such as a highly constrained device, products might be delivered with software pre-installed and no mechanism to re-install or update. **Ask**: Ask the developer to confirm that an administrator can verify the authenticity and integrity of software before it is installed, and that the details of how to do this are in the product's deployment guidance. **Action: Ensure that the product's deployment guidance makes clear how an administrator can verify the authenticity and integrity of software before it is installed. Ensure that details of how an administrator can verify the authenticity and integrity of a product's software before it is installed, are included in the Update Policy.**
Administrator authorised updates **CAPSS Ref 110**	**Threat: Installing compromised software using the update process** *Attackers may spoof update sources to deliver compromised software which provides them with access or control or disrupts a device's operation.* It is essential that software updates are validated and verified before installation. **Ask**: Ask the developer to confirm that any automatic software update procedure requires the update to have been authorised by the administrator before use. **Action: Ensure that the software update procedure requires the update to have been authorised by the administrator before use. If an automatic process is used, the product must be configured to authenticate updates. Ensure details are included in the Update Policy. Update Policy must also identify under what circumstances updates should be tested before being applied.**

Name	Description
Provide a configuration tool to enforce required settings **CAPSS Ref 300**	**Threat: Exploitation of an accidental misconfiguration** *Complex configurations, with multiple (often inter-related) options makes an accidental misconfiguration much more likely. If this results in insecure settings being configured the security of the product will be reduced and may remain undetected indefinitely.* If a software product requires more than 12 options to be changed or set by an administrator to configure it securely, a tool, policy template, or specific configuration guide is needed from the developer to help the administrator to reduce the likelihood of accidental misconfiguration. **Ask**: Ask the developer for guidance documentation on how to securely configure the product, and whether the initial configuration can be simplified using a supplied tool, policy template, or specific configuration guide. **Action**: Follow deployment guidance to perform initial configuration using any supplied tool, policy template, or specific configuration guide to achieve this in as few steps as possible.
Ensure product security configuration can only be altered by an authenticated system administrator **CAPSS Ref 301**	**Threat: Unauthorised alteration of product's configuration** *Compromise of the configuration of a product's security-enforcing settings will reduce the security of the product and may remain undetected indefinitely.* Security enforcing settings, including configuration of any key and certificate management required in support of authentication or other cryptographic functionality, need to be alterable only by authenticated administrators. **Ask**: Ask the developer to confirm that users must be authorised to change security-enforcing configuration settings. **Action**: Ensure that only authenticated administrators are authorised to change security-enforcing configuration settings.
Ensure product security configuration can be backed up **CAPSS Ref 302**	**Threat: Unauthorised alteration of product's configuration** *Compromise of a product configuration's security-enforcing settings reduces the security of the product. Even if compromise is suspected, it may be difficult to determine which (if any) settings have been altered and hence can take a significant time to correct, if the configuration is not readily restorable.* Backing up the product's security-enforcing settings enable them to be restored by an authorised administrator in a timely manner in the event of a failure or if they have been compromised. **Ask**: Ask the developer to confirm that the product has a means to securely backup its configuration, and to restore it when required. **Action**: Ensure that a Backup Policy has been defined that includes all products in use. Ensure that the administrator is advised how to use each product's features to securely backup their configuration and provided with guidance on the process of restoring the security configuration in a timely fashion in the event of a failure or compromise.

Name	Description
Role based access control **CAPSS Ref 500**	**Threat: Privilege escalation on management application, or unauthorised use of management privilege** *Unnecessarily elevated privileges increase the risk of both accidental and deliberate management changes, as well as making the privileges available to other software (including malware) executed by the user.* Role-based access control ensures that users, assigned a specific role, are only able to perform operations and access data appropriate to their role. **Ask**: Ask the developer whether the definition of user roles is customisable; if so, ask how it is authorised. **Action**: Enforce separate accounts for device management, account administration and user access, ensuring that users are only assigned roles necessary for their duties. If the definition of user roles is customisable, ensure that this customisation can only be performed by an admin user with appropriate privilege.

Case Study – Spear-phishing attack targets system administrator

It is essential to ensure that staff are aware of techniques used to obtain and use personal information in order to infiltrate an organisation. System administrators especially, as they have elevated privileges, should be aware that they are a particular target.

A system administrator within a high-profile UK organisation was successfully spear-phished and unknowingly installed a Remote Access Tool (RAT) allowing the attackers to obtain information about the network and systems. The attackers had identified the individual and their subjects of personal interest. They crafted a socially-engineered email to the administrator's personal email address. The administrator accessed personal webmail from the admin computer, read the phishing email and downloaded an infected document from a file sharing service containing the first stage malware. When the document was opened the user was prompted to run an executable, which breached defences and installed the malware onto the system. The attackers exploited poor security awareness by repeatedly requesting approval to run until the administrator finally clicked 'OK'. The malware communicated with domains controlled by the attackers and subsequently downloaded a second stage (the RAT). The attackers captured data and screenshots to learn more about the organisation's network and systems. After a week the data transfers were detected, the attackers' domains were blocked, and the machine was disconnected from the network for forensic analysis. Although the compromise was detected before any significant damage was done, the investigation and clean-up required resources and expertise and disrupted day-to-day operation of the organisation.

Although the compromise was eventually detected thanks to monitoring, the poor security awareness of the administrator enabled the attack, allowing open web browsing on the admin computer facilitated it, and the lack of malware protection in the network or the admin computer resulted in the failure to detect or block the malware at the time of the compromise.

Name	Description
User least privilege **CAPSS Ref 501**	**Threat: Taking advantage of existing user privilege** *If elevated privileges are required to use a product, any other software executed by that user (including malware) also has those elevated privileges.* Where a product is used for a non-admin role, it needs to operate correctly from a standard account without elevated privileges. **Ask**: Ask the developer to confirm that elevated privileges are not required to use the product. Ask for product deployment guidance to identify privileges required for each user role. **Action**: Ensure that unnecessary privileges are not assigned to users – applications should not be running as 'admin'.
User authentication **CAPSS Ref 502**	**Threat: Exploitation of weak user passwords or unattended workstations** *The use of weak passwords increases the risk of unauthorised access; leaving workstations unattended without locking the session also increases the risk of unauthorised access (either opportunistic or planned).* If users are not required to use an MFA authentication mechanism (that is unique to each user), a password policy needs to be enforced. User session must be locked-out if they have been inactive for a defined period. **Ask**: Ask the developer to confirm that a robust password policy (with discrete passwords per account) can be enforced. **Action**: Enforce the password policy is at least as robust as that in Appendix A. Require passwords to be changed upon suspicion that a password has been compromised. Previous passwords must not be allowed in case they have been compromised. Ensure that default passwords are changed at installation and that they are changed to passwords that comply with the password policy (see **Case Study – The developers backdoor** below).

Case study – The developer's backdoor

Management of the IT systems which support physical security controls is often outside the direct control of an organisation's IT functions and more often than not outside the visibility of the IT security department. This can mean that systems are not tested in the same way as corporate IT systems and as a result security weaknesses can exist. Often the systems are deployed by a 3rd party provider who uses their default or standard build which may include pre-installed user accounts for both the Operating System and physical security software.

During security testing of their physical security system, one organisation identified that the 3rd party support organisation had a 'backdoor' account across all their systems. The account had never been used to login but was set up on all systems and the password was the same on them all. With knowledge of the username and password this account could have been used to gain access to all systems on the physical security systems network, not only at this organisation but any other one managed by the same company. This highlights the importance of an installation and system maintenance programme that includes specific security enhancement activities.

Of most importance is identifying default and developer-installed accounts and altering passwords from default values.

Name	Description
One administrator per account **CAPSS Ref 503**	**Threat: Unauthorised use of an admin account** *Shared administrator accounts increase the risk of compromise, and do not provide sufficient accountability for administrative actions.* If more than one administrator is required (e.g. to provide suitable levels of cover to ensure that administrative actions can always be completed in a timely manner) then a separate admin account needs to be assigned per administrator. **Ask**: Ask the developer to confirm that the product supports two or more administrator accounts. **Action**: Ensure that two or more users are prohibited from using the same user account.

Physical protection

Name	Description
Disable non-operational physical interfaces **CAPSS Ref 200**	**Threat: Exploitation of insecure internal or external interfaces** *Interfaces that are not required for normal use could be used to undermine the device security, if they can be accessed by an attacker.* Interfaces that are not required for normal use need to be disabled. This includes debug interfaces within the device, physical interfaces such as external ports (USB, etc.) or internal removable media (such as SIM cards). **Ask**: Ask the developer to confirm what interfaces are available in the product (both internal and externally accessible), how they are disabled in normal use; and that the product's deployment guidance includes any administrator action required to disable interfaces. **Action: Ensure that any measures to disable interfaces that are identified in the product's deployment guidance have been implemented.**
Tamper response **CAPSS Ref 201**	**Threat: Access to structures inside the tamper-protection boundary of the device** *If an attacker can gain access to the internal components of a device, they may be able to gain control of the device and obtain sensitive data held within the device. If attempts to gain access are undetected the device could be under an attacker's control for a significant length of time.* Attempts to access the internal components of a device need to be deterred and detected, by detecting any breach of the tamper-protection boundary and causing an alert and log entry. The alert may be indicated by various means such as an alarm or flashing indicator or an alert raised at a connected controller when the connection is lost. If the tamper event is recorded in a log, some simple devices with memory constraints may treat the log as circular, causing older entries to be overwritten by the latest entry if the log is full; in this case the log needs to be capable of holding at least 100 entries and be exportable to another device regularly. End user devices that are protected by appropriate measures specified in [NCSC Mob] guidance to encrypt local data, such as Bitlocker, do not need to generate a tamper alert as long as their disconnection from a controller is alerted by the controller. **Ask**: Ask the developer to confirm that tamper alerts are generated and logged, and whether they can be transmitted to a central alert panel/workstation. If a log is used, then ask the developer to confirm that the log can contain at least 100 entries and whether there are any constraints affecting the size or availability of the alert log. **Action**: Ensure that procedures are in place to collect and monitor tamper alerts and take appropriate action. If the device's log is constrained, ensure that it is exported to another device (such as a controller or central logging facility) regularly enough that log entries are unlikely to be lost.

Name	Description
Fail secure on power loss **CAPSS Ref 202**	**Threat: Exploitation by removing power** *Power failure can be exploited if the device fails or restarts in a way that undermines the device's security.* **Ask**: Ask the developer to confirm the behaviour of the device on power loss; and that the product's deployment guidance includes any specific configuration that is required to ensure that it fails secure on power loss, and that it does not restart in a state that undermines security. **Action: Identify undesirable states or functions and ensure these are not achievable via loss of power or a power cycle of the device. If necessary, configure the device according to the product's deployment guidance to ensure that it fails secure on power loss, and does not restart in a state that undermines security.**
Protection of security-related physical structure **CAPSS Ref 203**	**Threat: Physical compromise of the device, unauthorised physical access to security-critical data stored on the device** *If an attacker can gain access to the internal components of a device, they may be able to gain control of the device and obtain sensitive data held within the device.* To protect against tampering with the internals of a device, all components that generate, process and store sensitive data (including cryptographic keys) need to be within the tamper-protection boundary, ensuring that they cannot be accessed without breach of the tamper-protection boundary. An opaque casing prevents inspection or visibility of the internal layout or components of the device. If tamper-evident measures are employed, attempts at tampering are detectable by physical inspection. End user devices that are protected by appropriate measures specified in [NCSC Mob] guidance to encrypt local data, such as Bitlocker, do not need a tamper-protection boundary. **Ask**: Ask the developer to confirm which devices need to be deployed in a secure area or secure enclave, and whether tamper-evident measures are included. **Action**: If no suitable tamper-evident measures are included in the devices, employ tamper-evident measures. To be suitable, such measures (for example, seals) must be of restricted availability or require the use of a special tool with restricted availability, to prevent an attacker successfully replacing one with a new, undamaged seal. Sites requiring more than a basic level of protection must use a CPNI approved tamper product (such as a CPNI Rated seal). Ensure that administrative staff regularly inspect devices for possible damage to tamper-evident measures and that any tampered device is removed from use immediately.

Name	Description
Physical security of management interfaces **CAPSS Ref 204**	**Threat: Physical compromise of management interfaces** *Unauthorised access to management interfaces can be used to remove or undermine security mechanisms.* Management interfaces are intended to be used to manage a device, including any security mechanisms and settings. The devices used for that interface must be protected against unauthorised access. **Ask**: Ask the developer to confirm that no end user devices that access management interfaces are required to be accessible in a non-secure area. **Action**: End user devices that are used to access management interfaces must not be accessible in a non-secure area. Admin access to subsystems that are deployed within the secure enclave, must also be within the secure enclave. Admin access to subsystems that are deployed outside the secure enclave but within a secure area, may be within the same secure area.

Data protection

Name	Description
Encrypt sensitive data **CAPSS Ref 105**	**Threat: Extraction of sensitive data held on the device** *Any data that is stored on a device is compromised if that device is stolen. Theft of a device containing unencrypted sensitive data may be the easiest way for an attacker to obtain that data.* Sensitive data (including personal data and configuration data) needs to be stored using encryption and integrity protection to ensure that the data is protected if the device is stolen. In general, sensitive data should not be stored on devices that are exposed outside of the secure enclave. **Ask**: Ask the developer to confirm that sensitive data held on a device is stored using encryption and integrity protection. **Action**: Configure devices containing sensitive data using mechanism such as Bitlocker or equivalents. Refer to [NCSC Mob] for specific guidance for end-user devices. Encryption of stored data must use AES with at least 128bit key. Ensure that procedural controls are defined to minimise the risks of compromise if devices that contain sensitive data are removed from the secure enclave (e.g. for specialist analysis).
Unique security data per device **CAPSS Ref 109**	**Threat: Gaining access to security data in a single device** *Security data that is shared across multiple devices can mean that the compromise of one device directly enables the compromise of other devices or provide a means for an attacker to masquerade as a different device.* To avoid this, devices need to contain no security data that can enable compromise of another device **Ask**: Ask the developer to confirm that security data is unique for each device. **Action**: Ensure that administrators do not assign common security data (such as passwords or keys) to multiple devices.

Name	Description
Encrypt communications traffic over untrusted link **CAPSS Ref 406**	**Threat: Interception of data from unencrypted links** *If an attacker can gain access to a communications link, they can eavesdrop on any data transmitted, and may also be able to intercept and modify data en route. Access may be gained by simply fitting a clamp over a cable (even fibre-optic) in a duct.* Any communications link that is partially or entirely outside the secure enclave must be regarded as untrusted and needs to use NIST approved cryptographic algorithms to protect traffic. Non-sensitive data in transit needs integrity protection at a minimum, while sensitive data must be encrypted, and integrity protected. **Ask**: Ask developer to confirm that communications links can be protected with suitable means. **Action**: Ensure that untrusted communications links are protected. Guidance on suitable means to protect data in transit can be found at [NCSC TLS] and [NCSC IPsec].

Malware protection

Name	Description
Deploy onto suitably protected endpoint **CAPSS Ref 303**	**Threat: Malware on endpoint** *Endpoints, such as a laptop or tablet, are the most common targets for attack and infection with malware to collect data (such as security credentials) or as an entry point into a network.* Endpoints need to be configured in line with good IT practice as defined in [NCSC Mob] Guidance. **Ask**: If the endpoint device is provided with the product, confirm that configuration guidance is provided that is equivalent to the relevant NCSC Mobile Device Guidance. **Action**: If the endpoint device is provided with the product, ensure that the provided configuration guidance is followed. If the endpoint device is not provided with the product, the relevant security guidance for end user devices provided at [NCSC Mob] must be followed where possible. Guidance is also provided in [NCSC Malware] to build defences against malware, in terms of preventing malicious code from being delivered to devices, preventing malicious code from being executed on devices, increasing resilience to infection and enabling rapid response should infection occur.

Case study – The malware outbreak

The systems that run and support physical security systems typically run Microsoft Windows Operating Systems; however, not all software developers are happy for anti-malware software to be installed on them. It is often assumed that if these systems are not connected to the internet they are not at risk of infection. As a result, the controls for detecting and removing malware are often not implemented and important security patches and upgrades are not applied. However, there are other routes through which malware can enter these environments, e.g. when an insecure support laptop is connected to the network or a USB drive is inserted into one of the PCs.

In one incident malware was introduced via removable media that was connected by a user to view holiday photos on the large screen in the control room. Putting aside the inappropriate use of the organisation's physical security systems, it was also subsequently determined that the user's USB stick contained malware. This spread by exploiting unpatched vulnerabilities in the Microsoft Windows Operating Systems that were running within the environment. Due to the infection the systems were rendered inoperable and all had to be taken offline to be rebuilt so that service could be restored. As a result of the incident the physical security systems were offline for 48 hours, creating significant disruption to operations and requiring additional overtime to be paid to the guard force. Despite the incident the developer of the equipment continues not to support the system if anti-malware software is installed and therefore a strict process has been implemented to prevent the introduction of further malware. However, the lack of anti-malware software sits as a significant item on the organisation's risk register.

This illustrates that even a segregated network that has no external connections can still be vulnerable to malware and measures need to be implemented to patch systems and protect against unauthorised connections. It also demonstrates the importance of ensuring that staff are not only aware of measures that are in place but also the threats that those measures are protecting the systems from.

Product quality

Name	Description
Evaluation / Cryptocheck **CAPSS Ref 100**	**Threat: Exploitation of a cryptographic algorithm implementation error** *Even if a strong cryptographic algorithm is used, a poor implementation may have flaws that can be exploited.* It is essential that only well-defined standard cryptographic algorithms are used in a product, including in communications protocols, and that the implementation of the algorithms has been independently validated as correct. Where a cryptographic algorithm is used within a communications protocol (e.g. TLS) then NCSC guidance should be followed in choosing the cryptographic algorithms and their parameters (e.g. [NCSC TLS]). Where no such guidance exists for the protocol, or where the cryptographic algorithm is being used outside of a communications protocol (e.g. for encrypting stored data) then best practice cryptography should be used, i.e. cryptography that is suitable for the corresponding use case and has no indications of a feasible attack with current readily available techniques[1]. Note that this does not refer only to the cryptographic primitives used, but also to the implementation, key generation and handling of keys. **Ask**: Obtain evidence (such as a CAVP certificate – see [NIST CAVP]) from the developer that the implementations of cryptographic algorithms in use have been independently validated. **Action**: Where a product offers a choice of algorithms, ensure that best practice cryptographic algorithms and key lengths/modes are selected as defined above (if in doubt seek advice from CPNI).
Heap hardening **CAPSS Ref 101**	**Threat: Exploitation of a software implementation/logic error** *Memory space is allocated dynamically for some purposes in software; there are many exploits employed by attackers that rely on poorly implemented memory management.* The management of memory allocation in software is vulnerable if not correctly implemented. That provided by an operating system is less likely to be flawed and more up to date to defend against the latest attacks than a bespoke approach implemented by a developer. **Ask**: Ask the developer to confirm that they either do not use a heap or that they use the heap memory management provided by the operating system.

[1] This definition is based on that in [ETSI EN303645].

Name	Description
Stack protection **CAPSS Ref 102**	**Threat: Exploitation of a software implementation/logic error** *If an attacker can cause a stack overflow or corruption (for example by sending a message that is too long) the control of the software is disrupted and can potentially be subverted.* The use of stacks in software is vulnerable if not correctly implemented. Stack protection is provided by most modern development tools and, when employed by the developer, protects against stack overflow and stack corruption, which is often used by hackers as a means of taking control of a software product. **Ask**: Ask the developer to confirm that they use the stack protection features of their development tools.
Data Execution Prevention **CAPSS Ref 103**	**Threat: Exploitation of a software implementation/logic error** *If an attacker is able to inject data into a device (through a vulnerability or a valid interface) that is actually executable code, it could be used to subvert the device.* Many modern platforms support Data Execution Prevention, to ensure that areas of memory that are intended to contain data cannot be executed as if they were code, an approach often taken by hackers to take control of a software product. **Ask**: Ask the developer to confirm that they use the Data Execution Prevention features of the underlying platform. **Action**: Ensure that administrators enable Data Execution Prevention when configuring devices.
Address Space Layout Randomisation **CAPSS Ref 104**	**Threat: Exploitation of a software implementation/logic error** *If software is always loaded at the same memory addresses an attacker will know where to look for sensitive data or vulnerable code.* Modern development tools support Address Space Layout Randomisation (ASLR) which ensures that software is not always loaded at the same memory addresses, making it harder for an attacker to know where to find specific data or code in the device's memory. **Ask**: Ask the developer to confirm that they have developed their product with full support for ASLR. **Action**: Ensure that administrators perform any required actions to enable ASLR when configuring devices.

Name	Description
Updateable product **CAPSS Ref 106**	**Threat: Exploitation of a known or discovered software implementation/logic error** *Once a vulnerability is discovered in a product, hackers will be looking to exploit it quickly before it has been patched. The longer it takes to apply a patch the longer the product is vulnerable.* Products need to be updateable to ensure that newly discovered flaws and vulnerabilities can be corrected in deployed installations. In some cases, such as a highly constrained device, updates may not be feasible. **Ask**: Ask the developer to confirm that the software in a device can be updated, and that the product's deployment guidance makes clear where and how an administrator is to be made aware of update availability and obtain them. **Action**: Ensure that administrators have defined and documented an Update Policy and that each product in use is included in it. For Critical vulnerabilities, the Update Policy must ensure that the update is applied within 14 days of becoming available.
Protected software environment **CAPSS Ref 108**	**Threat: Exploitation of a software implementation/logic error** *Hackers understand how to exploit vulnerabilities and flaws in software; if software hasn't been developed with an understanding of those potential flaws it may be vulnerable to standard attacks from hacking toolkits.* Developers are expected to implement software protection measures as part of their design and development process. This includes measures provided by the underlying platform or operating system, the use of development tools and analysis tools (such as static analysis to demonstrate compliance with MISRA 2012 rules for C), and development processes including code reviews to protect against known vulnerabilities and security flaws. **Ask**: Ask the developer to confirm what software protection measure they implement, and whether they can demonstrate compliance with MISRA 2012 rules for C (or equivalent).
Audit log review **CAPSS Ref 603**	**Threat: Exploitation of a software implementation/logic error** *An attack may result in a pattern of unusual events; if they are not logged and analysed the attack may go undetected and be repeated.* Log entries need to be regularly reviewed for unexpected entries. **Ask**: Ask the developer how the product enables review of audit logs. **Action**: Ensure that procedures are in place to regularly review log records for unexpected entries.

Name	Description
Vulnerability handling process CAPSS Pre-Requisite 4	**Threat: Exploitation of a software implementation/logic error** *If a vulnerability is discovered after release of a product and is not fixed within an appropriate time window, then it may be exploited by an attacker.* The developers must have a publicly stated vulnerability disclosure policy consistent with the recommendations in [ISO29147] and should have vulnerability handling processes consistent with [ISO30111]. **Ask**: Ask the developer for their written vulnerability handling process, and to confirm that this is consistent with [ISO29147] and [ISO30111].
Management system CAPSS Pre-Requisite 3	**Threat: Exploitation of a software implementation/logic error** *If the developers have a poor management system, insufficient quality assurance or lax version control, untested or flawed software may be installed by customers leading to exploitable vulnerabilities or unreliable systems.* The developers must provide evidence that they have a management system that encompasses information security. This can be demonstrated by [ISO9001] certification, and either [ISO27001] certification or Cyber Essentials PLUS [CEPlus] certification (or both). **Ask**: Ask the developer for evidence that their management system is compliant with [ISO9001], and either [ISO27001] or Cyber Essentials PLUS [CEPlus].

Monitoring

Name	Description
Log all relevant events **CAPSS Ref 600**	**Threat: Product usage that could be indicative of attacker activity** *An attack may result in a pattern of unusual events; if they are not logged for analysis the attack may go undetected and be repeated.* It is essential that logs (i.e. event and information logs) log all events that would be deemed of interest to an operator investigating a potential event or incident. **Ask**: Ask developer to confirm what events are logged and, if it is configurable, that details are included in the product's deployment guidance. **Action**: Configure products to log all actions deemed of interest; as a minimum: Authentication attempts Loss of connection with devices/loss of network connectivity (if available) Change of software or firmware versions Tamper events (if available) Change of configuration Change of time Deletion of logs (or log entries), including archiving of logs if this causes the deletion. Ensure that logs are, where possible, automatically exported to a management device in a secure area. Log entries must be assessed for impact following organisational procedures for incident resolution.

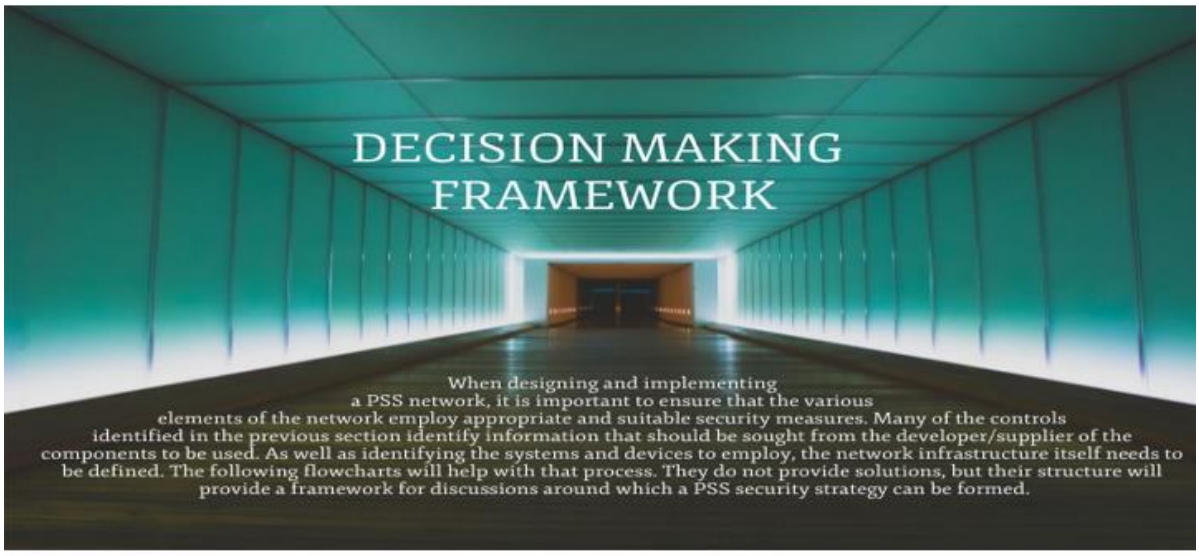
Name	Description
Protect access to logs **CAPSS Ref 601**	**Threat: Modification of logging generation, or sanitisation of illegitimate access from logs** *If logs can be modified, they could be altered by an attacker to remove evidence of an attack.* To counter this all log entries need to be time-stamped, and modification of log entries must not be possible. Where logs are of limited capacity an administrator needs to be alerted before logs are overwritten to provide sufficient opportunity for logs to be backed up or exported. **Ask**: Ask the developer to confirm that access to logs can be controlled. **Action**: Ensure that only an authenticated administrator can manage logs. Ensure that log timestamps are accurate and synchronised with a reliable time source.
Export logs **CAPSS Ref 602**	**Threat: Modification of locally stored logs** *If logs are not securely archived, they could be altered by an attacker to remove evidence of an attack.* To protect against loss of logs and modification of local logs, there needs to be a mechanism to transfer log records to an external device for archiving and analysis. Integrity of log records in transit needs to be protected. **Ask**: Ask the developer to confirm that there is a mechanism to automatically transfer logs to an external device, and that the integrity of the log records is protected in transit. **Action**: Ensure that the product is configured to automatically transfer logs to an external device and protect the integrity of the log records in transit.

Case study – Chain of custody

Monitoring logs often provides the first indication that an attack is underway. Collecting logs and analysing them can provide vital evidence that can distinguish between a simple failure and a systematic attack. But the integrity of the logs themselves is crucial to performing that analysis. One organisation collected logs from various systems at the end of each day and ran automated analysis overnight. However, an attacker had found a way of obtaining access to one of the systems and was able to remove log entries that would have drawn attention to their activities. They regularly accessed the system at night, collecting information, but always covering their tracks before the logs were collected for analysis. This extended hack only came to light one morning when the attacker was still connected and an administrator happened to notice an odd log entry on a system console. Making a note to consult the analysis of the logs they were subsequently surprised when the entry did not appear in the analysis report. After investigation over a few days it became clear that log entries were being removed. Eventually the compromised system was identified and the security breach fixed.

It is important to ensure the integrity of evidence such as logs being used to determine the security and status of a system.

Name	Description
Record when device last seen **CAPSS Ref 604**	**Threat: Product usage that could be indicative of attacker activity** *An attack may go undetected for some time if it starts by disabling devices that would otherwise detect the attack.* An attack may start with the disruption or removal of devices (such as sensors). A device such as a controller that has contact with other devices needs to be able to identify when it last had contact with another device. Where a device has not been seen for a period above a preset limit, a log record needs to be generated identifying the device that has not been seen. **Ask**: Ask the developer to confirm that the removal of a device can be detected (for example by a controller) within a defined time period. **Action**: Where the preset 'not seen' limits are configurable, ensure they are set to appropriate values depending on the type of device and appropriate periods of inactivity.



Green nodes on the flow chart are the start of the process

Orange nodes show decisions to be made

Blue nodes show the most secure solutions. Multiple blue nodes reflect the most secure solution for different scenarios

Red nodes show the less secure solutions

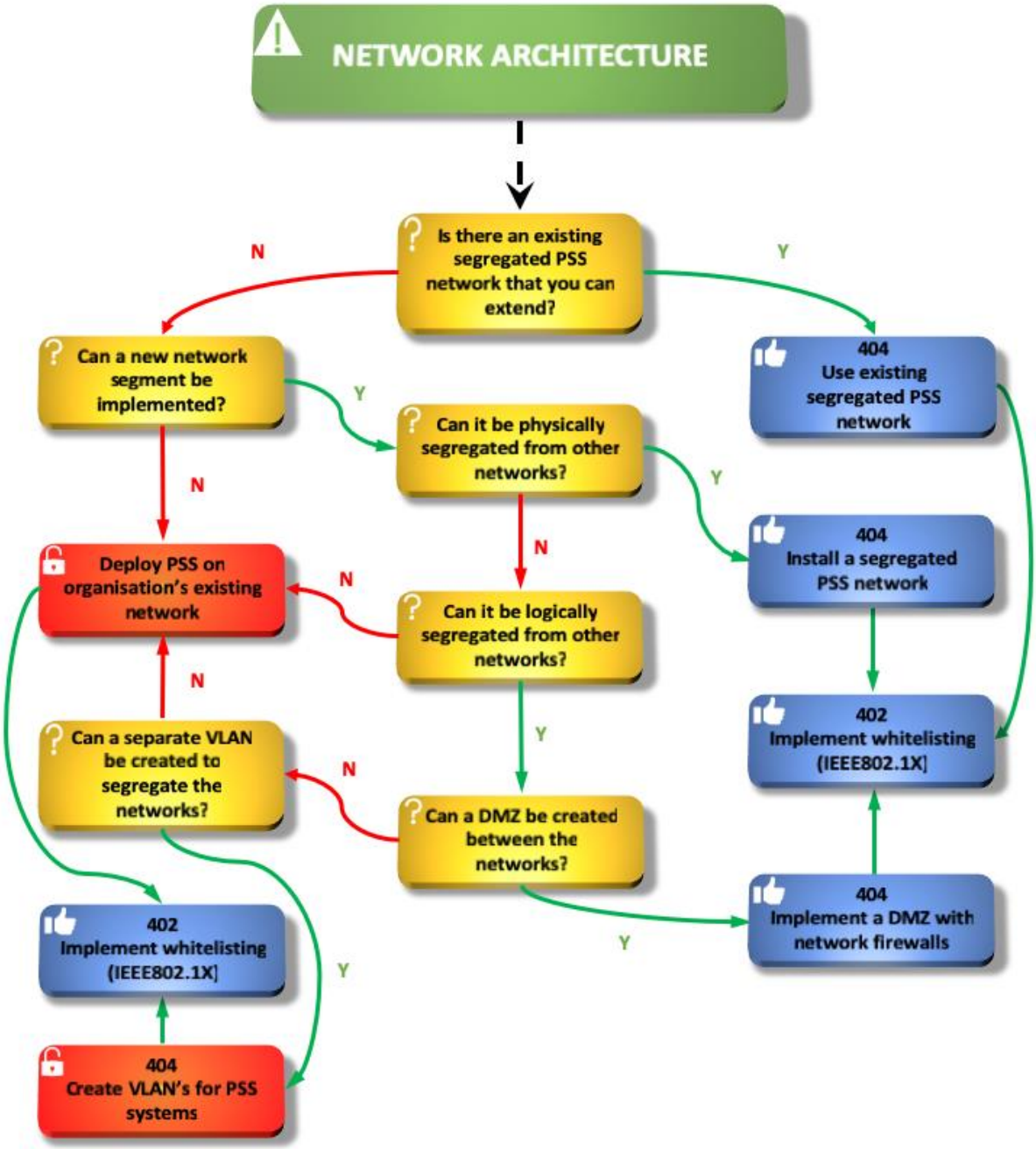
When applying a sites specific situation to the flowcharts below, the aim is to directly reach and implement, as many of the blue nodes as possible - this ultimately would lead to the "**ideal solution**".

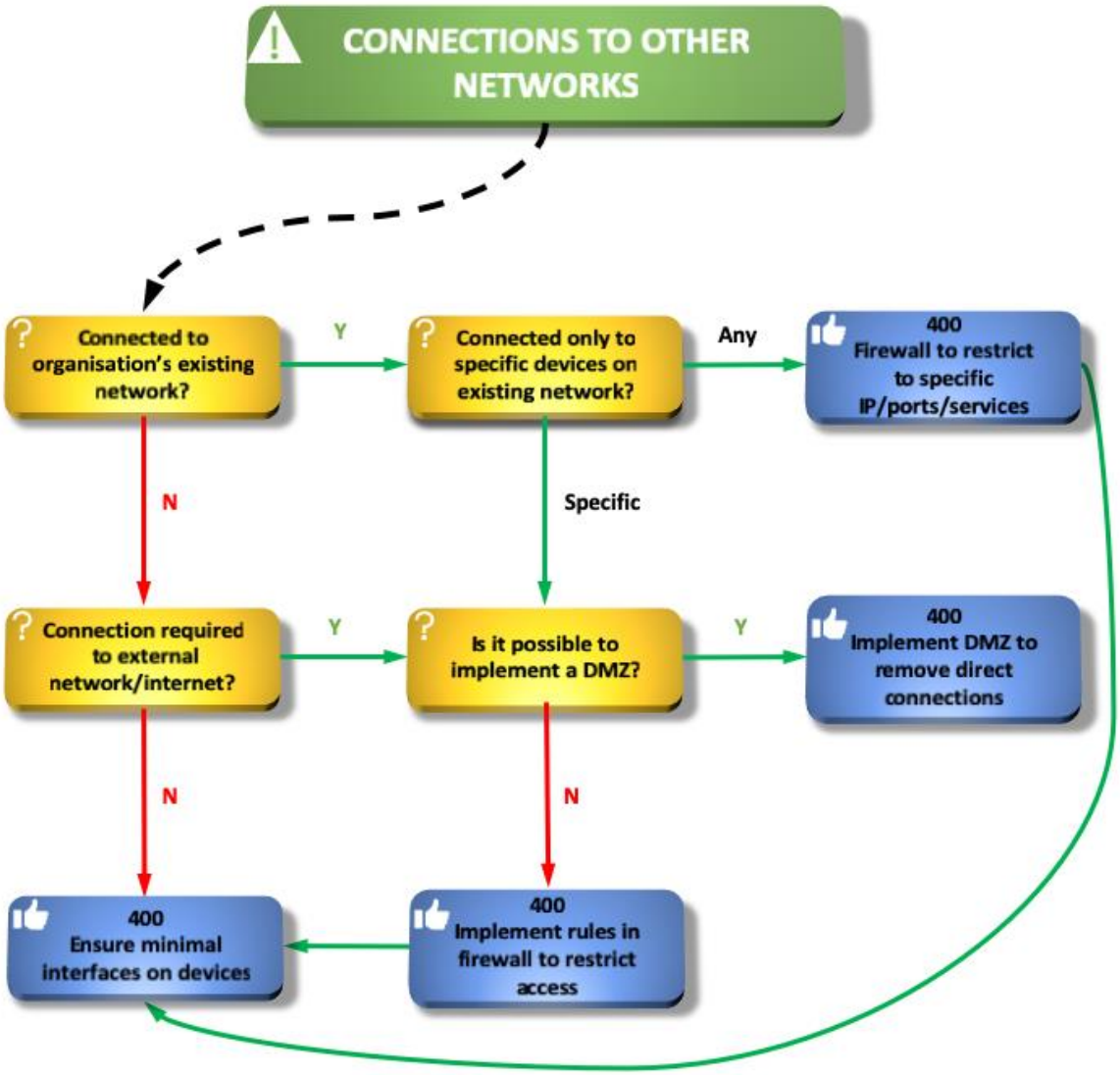
A situation may occur where traversing or ending up on a red node is the only option - this is the "less than ideal solution"

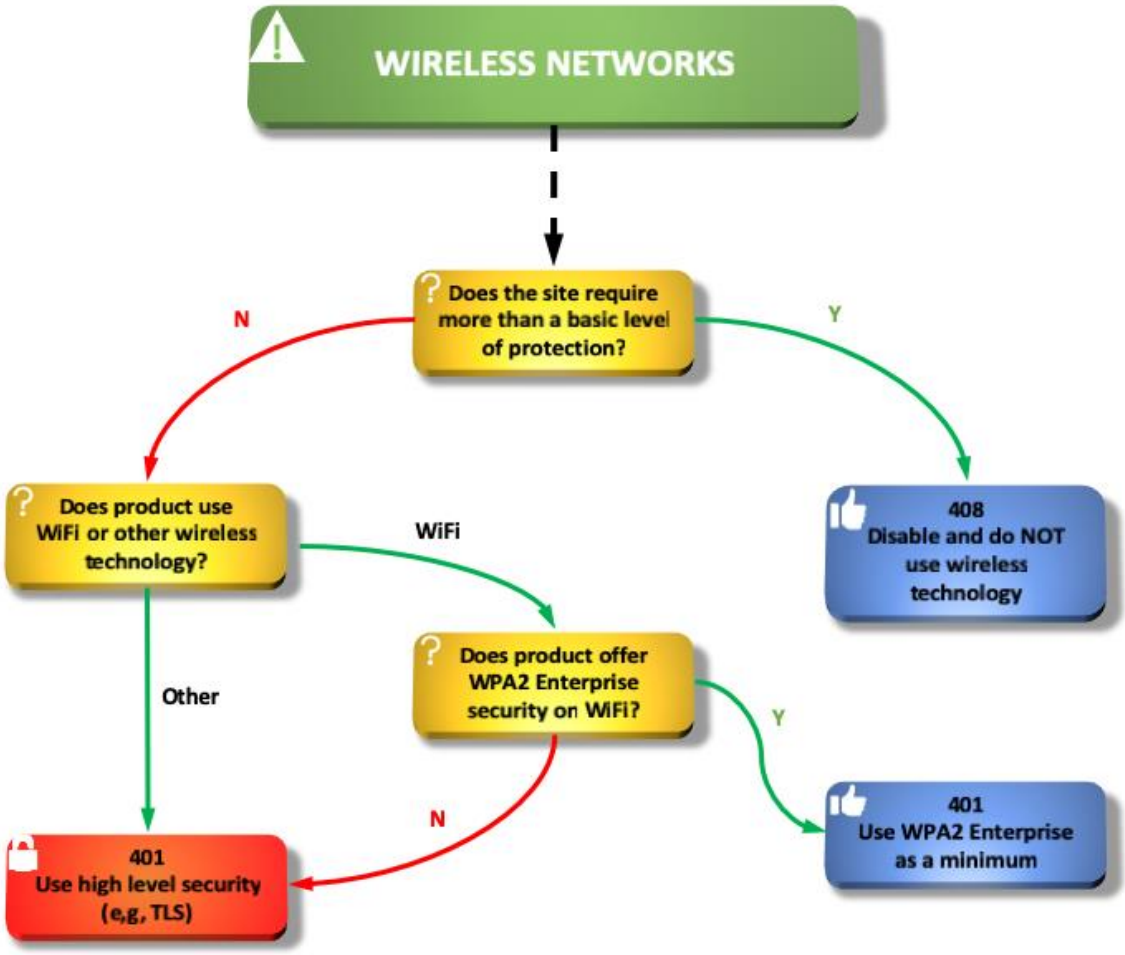
KEY POINTS

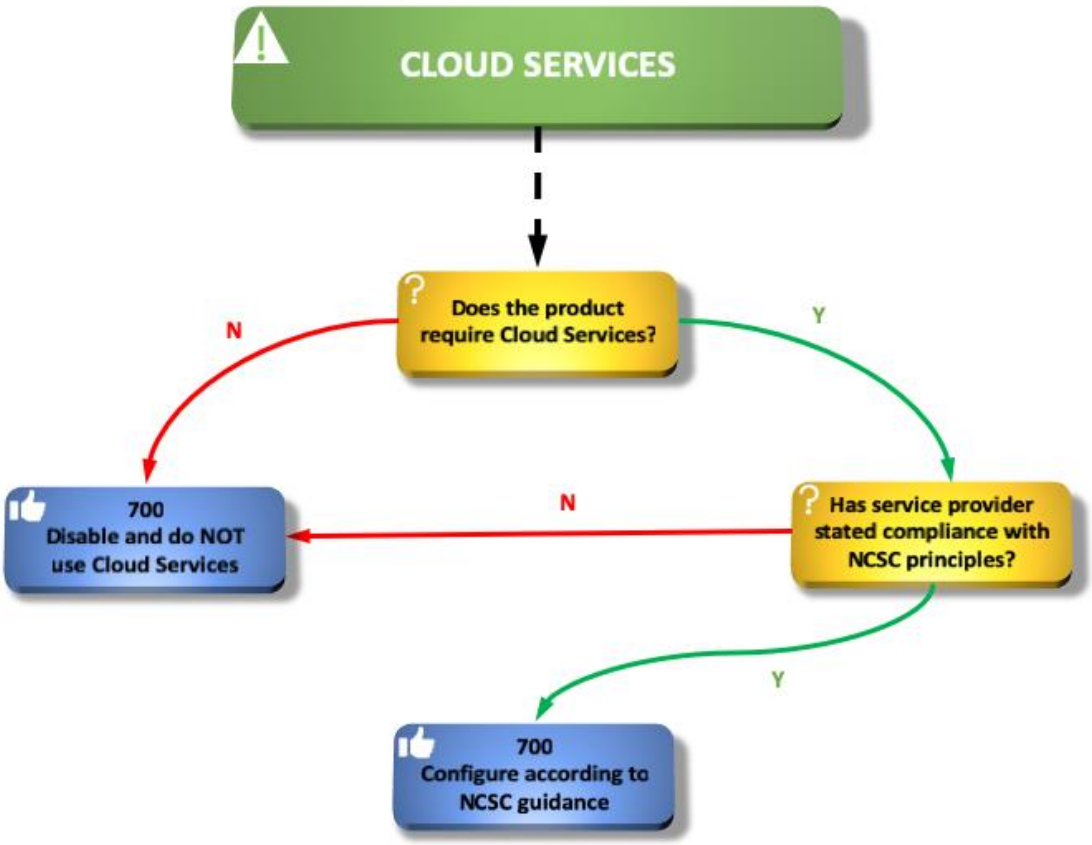
1. EVEN IN LESS THAN IDEAL SOLUTIONS A MITIGATION WILL STILL EXIST AND SHOULD BE IMPLEMENTED.

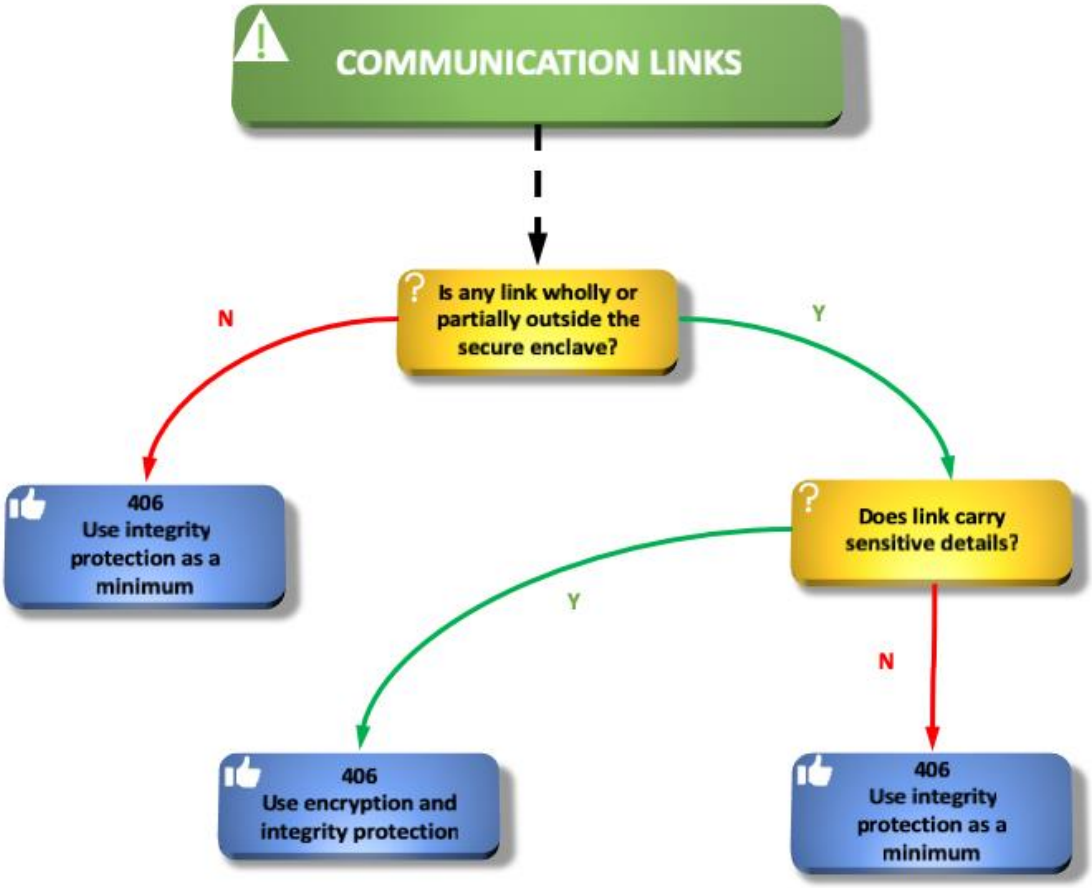
2. THE JOURNEY IS AS IMPORTANT AS THE END POINT

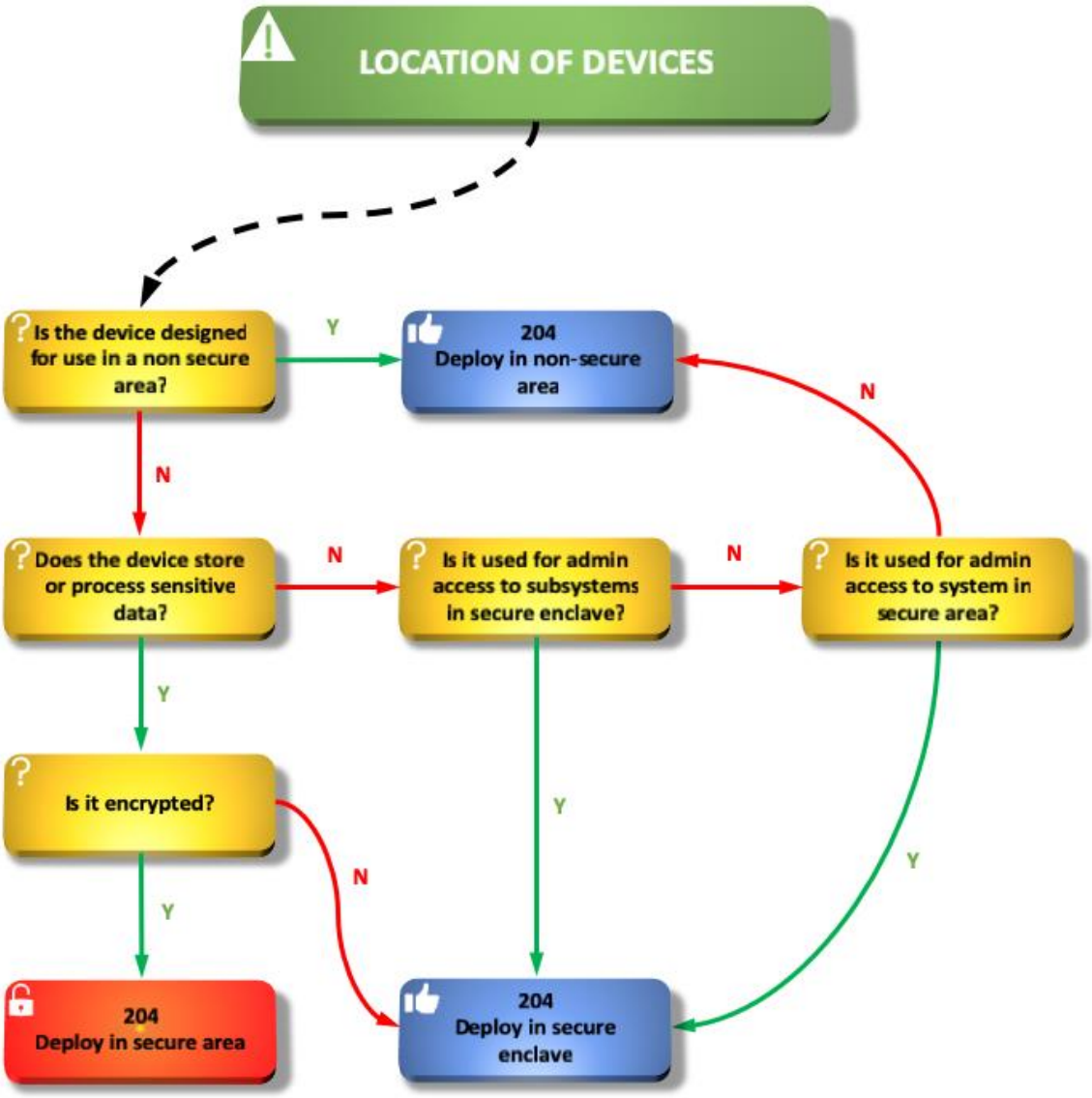

NETWORK ARCHITECTURE
Is there an existing segregated PSS network that you can extend?
N
Y
Can a new network segment be implemented?
404 Use existing segregated PSS network
Y
Can it be physically segregated from other networks?
N
Y
Deploy PSS on organisation's existing network
404 Install a segregated PSS network
N
Can it be logically segregated from other networks?
N
402 Implement whitelisting (IEEE802.1X)
N
Y
Can a separate VLAN be created to segregate the networks?
Can a DMZ be created between the networks?
N
404 Implement a DMZ with network firewalls
Y
Y
402 Implement whitelisting (IEEE802.1X)
404 Create VLAN's for PSS systems


CONNECTIONS TO OTHER NETWORKS
Connected to organisation's existing network?
Y
Connected only to specific devices on existing network?
Any
400 Firewall to restrict to specific IP/ports/services
N
Specific
Connection required to external network/internet?
Y
Is it possible to implement a DMZ?
Y
400 Implement DMZ to remove direct connections
N
N
400 Ensure minimal interfaces on devices
400 Implement rules in firewall to restrict access


WIRELESS NETWORKS
Does the site require more than a basic level of protection?
N
Y
Does product use WiFi or other wireless technology?
WiFi
Other
408
Disable and do NOT use wireless technology
Does product offer WPA2 Enterprise security on WiFi?
Y
N
401
Use WPA2 Enterprise as a minimum
401
Use high level security (e,g, TLS)


CLOUD SERVICES
Does the product require Cloud Services?
N
Y
700
Disable and do NOT use Cloud Services
N
Has service provider stated compliance with NCSC principles?
Y
700
Configure according to NCSC guidance


COMMUNICATION LINKS
Is any link wholly or partially outside the secure enclave?
N
Y
406 Use integrity protection as a minimum
Does link carry sensitive details?
Y
N
406 Use encryption and integrity protection
406 Use integrity protection as a minimum


LOCATION OF DEVICES
Is the device designed for use in a non secure area?
Y
204 Deploy in non-secure area
N
N
Does the device store or process sensitive data?
N
Is it used for admin access to subsystems in secure enclave?
N
Is it used for admin access to system in secure area?
Y
Y
Y
Is it encrypted?
N
Y
204 Deploy in secure area
204 Deploy in secure enclave

Glossary

AACS	Automated Access Control System
AD	Active Directory
BIOS	Basic Input / Output System – controls the hardware on a PC
CAVP	NIST Cryptographic Algorithm Validation Program
CCTV	Closed Circuit Television
CPNI	Centre for the Protection of National Infrastructure
DCMS	Department for Digital, Culture, Media and Sport
DMZ	De-Militarised Zone
DVR	Digital Video Recorder
Ethernet	Wired network
IP	Internet Protocol
IT	Information Technologies
LAN	Local Area Network
MAC	Media Access Control – a unique identifier for each network adapter
MFA	Multi-Factor Authentication
NIST	(US) National Institute of Standards and Technology
NCSC	National Cyber Security Centre
OS	Operating System
PSS	Physical Security System
SOC	Security Operations Centre
VLAN	Virtual Local Area Network

References

For the latest cyber security advice and information about vulnerabilities refer to the CPNI website, **www.cpni.gov.uk** .

[CPNI CAPSS] CPNI, *Cyber Assurance of Physical Security Systems (CAPSS) – 2019 Security Characteristic*, June 2019
https://www.cpni.gov.uk/system/files/documents/1b/33/CAPSS%202019%20-%20Security%20Characteristic%20V1.0%20%281%29.pdf

[CPNI CtrlRms] CPNI, *Control Rooms Guidance*, December 2016
https://www.cpni.gov.uk/system/files/documents/73/38/Control%20Rooms%20Guidance%20Dec%202016.pdf

[DCMS SbD] DCMS, *Secure by Design*, *Code of Practice for Consumer IoT Security*, June 2019
https://www.gov.uk/government/collections/secure-by-design

[ETSI EN303645] ETSI, Draft ETSI EN 303 645 *Cyber Security for Consumer Internet of Things*, November 2019
https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.00.00_20/en_303645v020000a.pdf

[IEEE802.1X] IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control, 2010,
https://standards.ieee.org/standard/802_1X-2010.html

[ISO29147] ISO, Information technology — Security techniques — Vulnerability disclosure, 2018,
https://www.iso.org/isoiec-27001-information-security.html

[ISO30111] ISO, Information technology — Security techniques — Vulnerability handling processes , 2019
https://www.iso.org/standard/69725.html

[MS Integrity] Microsoft, *Mandatory Integrity Control*
https://docs.microsoft.com/en-us/windows/win32/secauthz/mandatory-integrity-control

[MS Libraries] Microsoft, *Secure loading of libraries to prevent DLL preloading attacks*,
https://support.microsoft.com/en-us/help/2389418/secure-loading-of-libraries-to-prevent-dll-preloading-attacks

[MS SecuringAD] Microsoft, *Best Practices for Securing Active Directory*,
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

[NCSC CAF] NCSC, *Cyber Assessment Framework* v3.0, September 2019
https://www.ncsc.gov.uk/collection/caf

[NCSC Cloud] NCSC, *Cloud security guidance*, November 2018
https://www.ncsc.gov.uk/collection/cloud-security

[NCSC Common] NCSC, *Common Cyber Attacks: Reducing The Impact*, January 2016
https://www.ncsc.gov.uk/guidance/white-papers/common-cyber-attacks-reducing-impact

[NCSC IPsec] NCSC, *Using IPsec to protect data*, September 2016
https://www.ncsc.gov.uk/guidance/using-ipsec-protect-data

[NCSC Lateral] NCSC, *Preventing Lateral Movement*, February 2018
https://www.ncsc.gov.uk/guidance/preventing-lateral-movement

[NCSC Log] NCSC, *Introduction to logging for security purposes*, July 2018
https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes

[NCSC Malware] NCSC, *Mitigating Malware*, February 2018
https://www.ncsc.gov.uk/guidance/mitigating-malware

[NCSC Mob] NCSC, *Mobile Device Guidance*, January 2020
https://www.ncsc.gov.uk/collection/mobile-device-guidance
Note that this has now replaced the NCSC *End user device (EUD) security guidance* that is referenced in the CAPSS SC [CPNI CAPSS]

[NCSC Obs] NCSC, *Obsolete platforms security guidance*, May 2017
https://www.ncsc.gov.uk/guidance/obsolete-platforms-security-guidance

[NCSC Pwned] NCSC, *Suitable list of compromised passwords*, 2019
https://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordsTop100k.txt

[NCSC Reprov] NCSC, *End user device (EUD) security guidance: Factory reset and reprovisioning*
https://www.ncsc.gov.uk/collection/end-user-device-security/factory-reset-and-reprovisioning

[NCSC Router] NCSC, *UK Internet Edge Router Devices: Advisory*, November 2018
https://www.ncsc.gov.uk/information/uk-internet-edge-router-devices-advisory

[NCSC Servers] NCSC, *Serving up some server advice*, April 2019
https://www.ncsc.gov.uk/blog-post/serving-up-some-server-advice

[NCSC TLS] NCSC, *Using TLS to protect data*, December 2017
https://www.ncsc.gov.uk/guidance/tls-external-facing-services

[NIST Auth] NIST *Digital Identity Guidelines: Authentication and Lifecycle Management*, June 2017
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

[NIST BIOS] NIST, *BIOS Protection Guidelines for Servers*, August 2014.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-147B.pdf

[NIST CAVP] NIST, *Cryptographic Algorithm Validation Program*
https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program

[NIST Firewalls] NIST, *Guidelines on Firewalls and Firewall Policy*, September 2009.
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

[NIST ICS] NIST, *Guide to Industrial Control Systems (ICS) Security*, Revision 2, May 2015. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[NIST IDPS] NIST, *Guide to Intrusion Detection and Prevention Systems*, July 2012. https://csrc.nist.gov/publications/drafts/800-94-rev1/draft_sp800-94-rev1.pdf

[NIST KeyMan] NIST, Recommendation for Key Management: *Part 1: General*, January 2016 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

[NIST Log] NIST, *Guide to Computer Security Log Management*, September 2006. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

[NIST Patch] NIST, *Guide to Enterprise Patch Management Technologies*, Revision 3, July 2013. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

[NIST Sanitise] NIST, *Guidelines for Media Sanitization*, Revision 1, December 2014. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

[NIST Server] NIST, *Guide to General Server Security*, July 2008. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf

[NIST Storage] NIST, *Guide to Storage Encryption Technologies for End User Devices*, November 2007. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf

[NIST Telework] NIST, *User's Guide to Telework and Bring Your Own Device (BYOD) Security*, July 2016. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf

Appendix A - Minimum Acceptable Password Policy

The following requirements are identified in [CPNI CAPSS] as the minimum for an acceptable password policy.

- The system will require the user to change the password when logging in for the first time.
- The password must be a minimum of nine characters in length.
- The password must have a maximum length of at least 64 characters.
- Account lock out shall be set at ten attempts or less (min of three).
- Passwords must not be:
    - Passwords obtained from previous breach corpuses (by checking against an offline list obtained from a reliable source such as [NCSC Pwned]).
    - Dictionary words. (Where the whole password is a single dictionary words)
    - Three or more repetitive or sequential characters (e.g. 'aaa', '1234abcd').
    - Context-specific words, such as the name of the service, the username, and derivatives thereof.
- Passwords should only be required to be changed upon suspicion that a password has been compromised. No previous password shall be allowed by the product (because they're suspected to have been breached!)
- Passwords should be stored hashed and salted with a unique salt per password.

For systems with remote access, MFA should be used in line with NIST requirements [NIST Auth].

Appendix B - Checklist of questions to ask suppliers

Many of the controls identified in this document specify information that should be sought from the developer/supplier of the components to be used (under the **Ask** heading). These can be employed, for example, in an Invitation to Tender in order to facilitate decisions between competing products. For ease of reference for such purposes, suitable questions have been collated into the table below.

Control	Questions to ask supplier
Network	
Wireless network must be secured	What wireless technologies are implemented? If WiFi is implemented, does it support WPA2 Enterprise security?
Use whitelist to limit communications	Does the product provide a whitelist feature?
Use segregated networks	Does the product support the use of segregated networks?
General resource management	What is the device's behaviour in the event of large amounts of incoming network traffic?
Do not deploy wireless technology at sites requiring more than a basic level of protection	Can the product be deployed without the use of wireless technologies? If wireless technologies are present, can they be disabled?
Suitable cloud services	Does the product require the use of external cloud services? If so, can you provider a statement of how they meet the NCSC Cloud Security Principles? Is there a published response by the cloud service provider to the NCSC Cloud Security Principles?
Use time synchronisation	If time can be set directly on the device, can this only be performed by an authorised and authenticated administrator?
Synchronised event time-stamps	Does the product ensure that time stamps in logs are synchronised between all of its component devices, so that all logs are based on the same time?
Minimise interfaces	Can you confirm that there are no unnecessary ports or services available on the device that are not required for it to function? Are any administrator actions required to disable interfaces clearly identified in the product deployment guidance?
Disable non-operational logical interfaces	What interfaces are available in the product? How are they disabled if not required in normal use? Does the product's deployment guidance include any administrator action required to disable interfaces?

Control	Questions to ask supplier
Protocol robustness testing	Can you provide evidence that the protocol implementations on the product have been subjected to fuzz testing?
Local management authentication	Can an MFA authentication mechanism be employed for admin user accounts?
Remote management authentication	Can remote access be disabled unless it is specifically required? Can any remote management interface be protected by a secure protocol, such as IPsec, SNMPv3, TLS or SSH with MFA authentication? Are there any undocumented or unauthenticated developer-installed accounts?
Administration	
Provide a configuration tool to enforce required settings	Can you provide guidance documentation on how to securely configure the product? Can the initial configuration be simplified using a supplied tool, policy template, or specific configuration guide?
Ensure product security configuration can only be altered by an authenticated system administrator	Must users be authorised to change security-enforcing configuration settings?
Ensure product security configuration can be backed up	Does the product have a means to securely backup its configuration, and to restore it when required?
Secure software delivery	Can an administrator verify the authenticity and integrity of software before it is installed? Are details of how to do this in the product's deployment guidance?
Administrator authorised updates	Does any automatic software update procedure require the update to have been authorised by the administrator before use?
Role based access control	Is the definition of user roles customisable? If so, ask how is it authorised?
User least privilege	Are elevated privileges required to use the product? Does the product deployment guidance identify privileges required for each user role?
User authentication	Can a robust password policy be enforced?
One administrator per account	Does the product support two or more administrator accounts?
Physical protection	
Tamper response	Are tamper alerts generated and logged? Can they be transmitted to a central alert panel/workstation? If a log is used, can the log contain at least 100 entries? Are there any constraints affecting the size or availability of the alert log?

Control	Questions to ask supplier
Protection of security-related physical structure	Which devices need to be deployed in a secure area or secure enclave? Are tamper-evident measures included?
Fail secure on power loss	What is the behaviour of the device on power loss? Does the product's deployment guidance include any specific configuration that is required to ensure that it fails secure on power loss, and that it does not restart in a state that undermines security?
Disable non-operational physical interfaces	What interfaces are available in the product (both internal and externally accessible)? How they are disabled if not required for normal use? Does the product's deployment guidance include any administrator action required to disable interfaces?
Physical security of management interfaces	Are any end user devices that access management interfaces required to be accessible in a non-secure area?
Data protection	
Encrypt sensitive data	Is sensitive data held on a device stored using encryption and integrity protection?
Unique security data per device	Is security data unique for each device?
Encrypt communications traffic over untrusted link	Can communications links be protected with suitable means?
Malware protection	
Deploy onto suitably protected endpoint	If the endpoint device is provided with the product, is configuration guidance provided that is equivalent to the relevant NCSC Mobile Device Guidance?
Product quality	
Evaluation / Cryptocheck	Can you provide evidence (such as a CAVP certificate) that the implementations of cryptographic algorithms in use have been independently validated?
Heap hardening	Does the product use a heap? If so, does it use the heap memory management provided by the operating system?
Stack protection	Does the product use the stack protection features of the development tools?
Data Execution Prevention	Does the product use the Data Execution Prevention features of the underlying platform?
Address Space Layout Randomisation	Has the product been developed with full support for ASLR?

Control	Questions to ask supplier
Updateable product	Can the software in the device be updated? Does the product's deployment guidance make clear where and how an administrator is to be made aware of update availability and how to obtain them.
Protected software environment	What software protection measures are implemented? Can the product demonstrate compliance with MISRA 2012 rules for C (or equivalent)?
Audit log review	How does the product enable review of audit logs?
Vulnerability handling process	Do you have a publicly stated written vulnerability handling process? Is it consistent with [ISO29147] and [ISO30111]?
Management system	Do you have a management system that is compliant with [ISO9001], and either [ISO27001] or Cyber Essentials PLUS [CEPlus]?
Monitoring	
Log all relevant events	What events are logged? If it is configurable, are details included in the product's deployment guidance?
Protect access to logs	Can access to logs be controlled?
Export logs	Is there a mechanism to automatically transfer logs to an external device? Is the integrity of the log records protected in transit?
Record when device last seen	Can the removal of a device be detected (for example by a controller) within a defined time period?