ITHealth

The ITHealth Assurance Dashboard and the NIS Regulations

Introduction

The NIS Regulations (Network and Information Systems Regulations 2018) place legal obligations on providers to protect UK critical services by improving cyber security. The regulations apply to two main groups: OES (operators of essential services) and DSPs (digital service providers). NHS healthcare is considered an essential service; so NHS Trusts and Foundation Trusts are designated as 'operators of essential services' and must comply with the requirements of the regulations. Failure to do so could result in a loss of service and regulatory action. This document outlines how ITHealth's Assurance Dashboard Solution helps NHS Trusts to manage their compliance to the NIS Regulations.

Background

The Directive on security of network and information systems (NIS Directive) is an EU-wide directive that focuses on the availability of crucial network and information systems in order to protect the union's critical infrastructure and thereby ensure service continuity. This Directive was transposed into UK law as The Network and Information Systems Regulations 2018 (NIS Regulations) on 10 May 2018.

The regulations help ensure UK operators in electricity, transport, water, energy, health and digital infrastructure are prepared to deal with the increasing number of cyber threats.

As the NIS Regulations came into effect before the UK leaves the EU, the UK government has confirmed that the Regulations will apply irrespective of Brexit.

The regulations apply to these two groups:

- Operators of Essentials Services (OES)
- Digital Service Providers (DSPs)

NHS healthcare is an essential service, so NHS Trusts and Foundation Trusts fall into 'Operators of Essential Services'.

Guiding cyber security principles and objectives

One of the key objectives of the NIS Regulations is to ensure that OESs take appropriate and proportionate technical and organisational measures to manage the risks to the security of network and information systems which support the delivery of essential services.

As such, the UK government has taken the approach of setting out 14 broad, outcomes-based guiding cyber security principles, rather than prescriptive rules. These fall under four top-level objectives as detailed below:

OBJECTIVE A

MANAGING SECURITY RISK

- A1. Governance
- A2. Risk management
- A3. Asset management
- A4. Supply chain

OBJECTIVE B

PROTECTING AGAINST CYBER ATTACK

- B1. Service protection policies and procedures
- B2. Identity and access control
- B3. Data security
- B4. System security
- B5. Resilient networks and systems
- B6. Staff awareness and training

OBJECTIVE C

DETECTING CYBER SECURITY INCIDENTS

- C1. Security monitoring
- C2. Proactive security event discovery

OBJECTIVE D

MINIMISING THE IMPACT OF CYBER SECURITY INCIDENTS

- D1. Response and recovery planning
- D2. Lessons learned

The Cyber Assessment Framework (CAF)

OES' compliance with the NIS Regulations' guiding principles are monitored through audits conducted by designated competent authorities (CAs). The National Cyber Security Centre (NCSC) has worked with government departments and CAs to develop a Cyber Assessment Framework (CAF) intended to help carry out effective security assessments. The CAF is based on structured sets of Indicators of Good Practice (IGPs) which fall within the 14 guiding principles.

ITHealth Assurance Dashboard Solution

ITHealth's Assurance Dashboard increases visibility of an NHS organisation's network to help better manage vulnerabilities, remediation and compliance. It consolidates all key cyber security information into a single, near real-time dashboard - giving complete, at-a-glance visibility of an NHS organisation's entire network and systems. Tailor-made for the NHS, with the NHS, the Dashboard features reports that are pertinent to NHS cyber set-ups and which increase understanding of risks within an NHS network, including levels of compliance at both a local and NHS Digital level. Customers have access to ITHealth's experienced and purely NHS focussed technicians who continuously offer best-practice advice. In addition, monthly assurance reports are provided by ITHealth which include concise summaries of the dashboard's information. These regular reports facilitate dissemination of key cyber and compliance information to the board and other relevant stakeholders. Almost all information within the Assurance Dashboard is drillable and exportable meaning network queries can be more quickly answered and dynamic worklists easily created. Ultimately, the Assurance Dashboard Solution provides Trusts with justified confidence in their cyber and compliance assurance - at all times.

> "Our aim was to get a simpler and more independent view of the state of our IT estate to better manage vulnerabilities and assure customers. What we actually got was so much more."
>
> MIKE PRESS, Chief Technical Officer, Nottinghamshire Health Informatics Service (NHIS)

Helping achieve compliance to the CAF

ITHealth's Assurance Dashboard Solution helps Trusts achieve compliance with the Cyber Assessment Framework. It isn't a panacea for the CAF, but it does help address a significant number of areas (supporting over 36 IGPs) which enables vital cost and time-savings. Importantly, it frees up resource that would otherwise be used by Trusts to manage these areas of compliance. The tables that follow include detail of which parts of the CAF and Indicators of Good Practice - that are expected to be achieved - that the Assurance Dashboard solution addresses. (*NB: the principles, objectives and indicators of good practice as featured within the tables have been taken from NCSC Guidance as published on the NCSC website on 15th November 2018.)*

A1. Governance

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

CAF Objective	CAF Indicator of Good Practice	How the Assurance Dashboard helps
A1.a Board Direction	*Regular board discussions on the security of network and information systems supporting the delivery of your essential service take place, based on timely and accurate information and informed by expert guidance.*	The Assurance Dashboard displays information on the security state of your entire network and systems in near real-time, so the security state of the network can always be accessed. ITHealth provides regular snapshot reports which facilitate board discussions. The reports highlight key trends, risks, and changes in the network, as well as demonstrate progress over time.

CAF Objective	CAF Indicator of Good Practice	How the Assurance Dashboard helps
A1.b Roles and responsibilities	*Appropriately capable and knowledgeable staff fill those roles and are given the time, authority, and resources to carry out their duties.*	Having the Assurance Dashboard as an available resource ensures that staff members have complete visibility of what's happening in the network to enable appropriate duties to be carried out effectively.
A1.c Decision-making	*Risk management decision-making is delegated and escalated where necessary, across the organisation, to people who have the skills, knowledge, tools, and authority they need.*	The Assurance Dashboard Solution regularly scans so it provides to senior management up-to-date information on the network and at-a-glance visibility of the risks that exist. This ensures that the correct and appropriate information is always available to facilitate risk management decision-making. The ITHealth team can also provide expert advice to Trusts to ensure that all possible information is available before a risk management decision is made. Additionally, as the Assurance Dashboard is dynamic it enables Senior Management to see the effect of decisions made in near real-time and therefore make any necessary changes to the decision promptly.
	Risk management decisions are periodically reviewed to ensure their continued relevance and validity.	As the Assurance Dashboard reguarly scans, it provides up-to-date information on risks that exist within the network. It makes it possible to continually monitor the impact of risk management decisions and so review whether these risk management decisions remain effective over time. As the Assurance Dashboard is constantly updated with the latest threat information, it also ensures that Trusts have the most relevant and valid information upon which to base risk management decisions.

A2. Risk Management

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

CAF Objective	CAF Indicator of Good Practice	How the Assurance Dashboard helps
A2.a Risk Management Process	*Your organisational process ensures that security risks to networks and information systems relevant to essential services are identified, analysed, prioritised, and managed.*	The Assurance Dashboard has been designed for this very purpose - to provide you with a holistic view of your estate and show you at-a-glance visibility of security risks and vulnerabilities that exist on your network. It flags priority areas for remediation and provides you with dynamic, actionable worklists. As the information is displayed in near real-time, you can monitor progress closely as changes within the network are made.

CAF Objective	CAF Indicator of Good Practice	How the Assurance Dashboard helps
A2.a Risk Management Process *(continued)*	*Your risk assessments are based on a clearly understood set of threat assumptions, informed by an up-to-date understanding of security threats to your essential service and your sector.*	The Assurance Dashboard is designed to simplify the process of compliance to sector-specific NHS Digital CareCERT alerts – automating much of the process. It will provide a continuous update of where CareCERT alerts have been fully addressed (resolved), and where issues remain outstanding. At all times, you will be aware of your CareCERT compliance levels and the number of devices within your network that remain vulnerable to a threat as identified within a CareCERT. In addition, ITHealth also keeps abreast of the threat landscape and can input new threat detail that may pose an issue to Trusts. This would quickly expose any potential impact and highlight vulnerable areas that require addressing.
	Your risk assessments are informed by an understanding of the vulnerabilities in the networks and information systems supporting your essential service.	The Assurance Dashboard provides complete visibility of what's happening in the network, so you can easily identify all systems connected to essential services. The Assurance Dashboard analyses all vulnerabilities that exist on these systems and so this information is then able to inform risk assessments on the supporting infrastructure.
	Your risk assessments are dynamic and updated in the light of relevant changes which may include technical changes to networks and information systems, change of use and new threat information.	The Assurance Dashboard gives Trusts a near real-time view of all devices on the network and the vulnerabilities that such devices are exposed to. ITHealth monitor the threat landscape to ensure that the latest threat information is used in the vulnerability scanning - giving Trusts the most up-to-date security position of all their devices. Having this near real-time information ensures that Trusts are able to perform dynamic risk assessments on the security of the network and quickly react and implement any changes that are required.
A2.b Assurance	*You validate that the security measures in place to protect the networks and information systems are effective and remain effective for the lifetime over which they are needed.*	The Assurance Dashboard gives Trusts a view of the security posture of the entire network and systems and so validates if your security measures are effective. It will show if, and when, there are security deficiencies and flag these as priority areas for remediation. These security deficiencies can act as an indicator that certain measures may no longer be effective and therefore need to be reviewed.
	You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of essential services.	The Assurance Dashboard gives Trusts a single method to gain assurance of the security of the entire network, including the essential services. ITHealth ensures that Trusts understand how the Assurance Dashboard works and remains available to answer questions regarding anything that is identified on the network.

CAF Objective	CAF Indicator of Good Practice	How the Assurance Dashboard helps
A2.b Assurance *(continued)*	*Your confidence in the security as it relates to your technology, people, and processes can be justified to, and verified by, a third party.*	The Assurance Dashboard provides empirical proof and demonstrates an organisation's compliance, rather than relying on manual systems and/or spreadsheets (which only leave room for potential error and guesswork). The Assurance Dashboard effectively acts as an independent witness to the estate and enables an ongoing confidence in cyber and compliance assurance. As the solution is supported by ITHealth, ITHealth also act as third-party verification.

A3. Asset Management

Principle - *Everything required to deliver, maintain or support networks and information systems for essential services is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).*

CAF Objective	CAF Indicator of Good Practice	How the Assurance Dashboard helps
A3.a Asset management	*All assets relevant to the secure operation of essential services are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date.*	The Assurance Dashboard continuously scans all IP addressable assets linked to the network and provides a granular level of detail for each asset identified. The Assurance Dashboard presents information in near real-time, so it ensures that Trusts always have an up-to-date inventory of network assets.
	Assets relevant to essential services are managed with cyber security in mind throughout their life-cycle, from creation through to eventual decommissioning or disposal.	The Assurance Dashboard displays all assets linked to the Trust's network and so helps identify which of these assets are relevant to essential services. The Assurance Dashboard enables Trusts to monitor the patch status of all essential services' assets to ensure that these assets remain up to date with relevant patches. The Assurance Dashboard is able to regularly perform vulnerability scans on the essential services' assets to ensure that the configuration is secure. If it is not, the Assurance Dashboard identifies the areas that need to be addressed to ensure that the appropriate changes are made to ensure the highest levels of cyber security are maintained.

B1. Service Protection Policies and Processes

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

CAF Objective	CAF Indicator of Good Practice	How the Assurance Dashboard helps
B1.a Policy and process development	*Your systems are designed so that they remain secure even when user security policies and processes are not always followed.*	The Assurance Dashboard presents a complete picture of the network and always exposes current system risks. This enables systems to be set-up using the most secure configuration possible. The Assurance Dashboard also allows Trusts to see the privileges that users have and ensure that these privileges are appropriate for each user. Ensuring that configurations are secure and users have the correct level of privilege minimises the damage that can be done by a user who doesn't follow the security policies and procedures.

B2. Identity and Access Control

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

CAF Objective	CAF Indicator of Good Practice	How the Assurance Dashboard helps
B2.a Identity verification, authentication and authorisation.	*The list of users with access to networks and systems supporting and delivering the essential service is reviewed on a regular basis, at least every six months.*	The Assurance Dashboard identifies all users with an admin account. This information can then be used to identify which of these users have access to the networks and systems supporting the essential service. The list is a dynamic view of these accounts making regular reviews easy to perform.
B2.b Device management	*You either obtain independent and professional assurance of the security of third-party devices or networks before they connect to your systems, or you only allow third-party devices or networks dedicated to supporting your systems to connect.*	Vulnerability scanning of devices is included as part of the Assurance Dashboard Solution. This scanning can be extended to include third-party devices before they connect to the network. The Trust will be provided with a full report demonstrating the vulnerabilities that exist on the devices. The reports are delivered by ITHealth giving independent and professional assurance of the security of these devices.

CAF Objective	CAF Indicator of Good Practice	How the Assurance Dashboard helps
B2.b Device management *(continued)*	*You perform regular scans to detect unknown devices and investigate any findings.*	The Assurance Dashboard continuously scans the network to identify a full, near real-time network asset inventory. The scan picks up both known and unknown devices on the network, so Trusts can easily investigate any 'unknown' devices found.
B2.c Privileged user management	*Privileged user access rights are regularly reviewed and always updated as part of your joiners, movers and leavers process.*	The Assurance Dashboard gives visibility of Administrator and Domain logins and will support awareness of privileged users and related access; these can be reviewed 24/7/365. In addition, the Assurance Dashboard gives visibility of Active Directory accounts and related information.
B2.d Identity and Access Management (IdAM)	*All user access is logged and monitored.*	The Assurance Dashboard tracks all user activity and user trends over time. It will provide alerts for users that haven't been seen on the network in the last 60 and 90 days, failed log-on attempts, users where passwords remain unchanged, new users on the network and all users who have domain admin privileges.
	Attempts by unauthorised users to connect to your systems are alerted, promptly assessed and investigated.	The Assurance Dashboard reports and alerts on failed logons. A spike in failed logons could be a symptom of a brute force attack on a system. Such alerts can be fully investigated using the data within the Assurance Dashboard.

B4. System Security

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

CAF Objective	CAF Indicator of Good Practice	How the Assurance Dashboard helps
B4.b Secure configuration	*You have identified, documented and actively manage (e.g. maintain security configurations, patching, updating according to good practice) the assets that need to be carefully configured to maintain the security of the essential service.*	The Assurance Dashboard shows the patching status of all devices linked to the network, so you can see at-a-glance which assets are up to date with patching and which still require updates. The Assurance Dashboard is also able to perform vulnerability scans on assets. The scan will show any vulnerabilities that exist on these devices and the remediation that is required to ensure a secure configuration is achieved.

CAF Objective	CAF Indicator of Good Practice	How the Assurance Dashboard helps
B4.b Secure configuration *(continued)*	*All platforms conform to your secure, defined baseline build, or the latest known good configuration version for that environment.*	The Assurance Dashboard solution includes vulnerability scans on the gold builds of both desktops and servers. The findings of these scans are reported back to the Trust in a format designed to make the remediation process as swift as possible. This ensures that all new devices are put onto the network with a secure configuration. Having a defined secure build enables Trusts to ensure that all devices on the network conform to these standards. The Assurance Dashboard collects information such as software version, patch status and operating system. This information is fully searchable making it easy to identify and remediate machines that are not conforming to the baseline build.
	You regularly review and validate that your network and information systems have the expected, secured settings and configuration.	The Assurance Dashboard provides a complete picture of the entire IT estate which can be accessed at-a-glance and in near real-time 24/7/365. It highlights all existing vulnerabilities within the network and flags these for remediation. It does this by way of reports that have been specifically designed to highlight key security information, e.g. Windows Updates, AV and encryption status for all desktops and servers, devices set with default passwords, vulnerabilities against a standard gold image, etc.
	Only permitted software can be installed and standard users cannot change settings that would impact security or business operation.	The Assurance Dashboard performs a full software inventory identifying every piece of software on the network. With the Assurance Dashboard, Trusts can easily identify unauthorised software that has been installed as well as set alerts for future unauthorised software installs.
B4.d Vulnerability Management	*Announced vulnerabilities for all software packages, network equipment and operating systems used to support your essential service are tracked, prioritised and mitigated (e.g. by patching) promptly.*	Nearly every time NHS Digital issues a CareCERT alert the detail is placed within the Assurance Dashboard which rapidly exposes the level of risk and allows Trusts to quickly and easily identify the number of affected devices within the network. The Assurance Dashboard provides a live update of where CareCERT alerts have been fully addressed (resolved), and where issues remain outstanding, so Trusts are aware of their CareCERT compliance levels at all times. The risk level associated with each CareCERT vulnerability is also shown in the Assurance Dashboard enabling the Trust to prioritise which vulnerabilities to address first. *(Continued on page 10...)*

CAF Objective	CAF Indicator of Good Practice	How the Assurance Dashboard helps
B4.d Vulnerability Management *(continued)*	*(... continued from page 9.)*	In addition, the CareCERT view within the Assurance Dashboard is a dynamic view; so if, for example, there is a CareCERT alert which has been resolved by the Trust but a machine then comes back onto the network with this vulnerability the CareCERT will go back into the unresolved list. This change of status can be alerted to ensure that this vulnerability is resolved as quickly as possible. Please note, if bespoke or rare solutions are in place at a Trust to support the delivery of essential services, then these may not be covered by NHS Digital's CareCERT alerts.

B5. Resilient Network and Systems

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

CAF Objective	CAF Indicator of Good Practice	How the Assurance Dashboard helps
B5.a Resilience preparation	*You use your security awareness and threat intelligence sources, to make immediate and potentially temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware.*	In the case of an event such as a widespread malware outbreak ITHealth would update the Assurance Dashboard to include information around devices that are vulnerable to this. This makes the process of temporary security changes a quicker and easier process as Trusts are in possession of the facts to know how the outbreak event is going to affect their network.

C1. Security Monitoring

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

CAF Objective	CAF Indicator of Good Practice	How the Assurance Dashboard helps
C1.a Monitoring coverage	*Monitoring is based on an understanding of your networks, common cyber attack methods and what you need awareness of in order to detect potential security incidents that could affect your essential service. (e.g. presence of malware, malicious emails, user policy violations).*	The Assurance Dashboard continually monitors the network and will provide visibility and awareness of cyber related attacks, ensuring that any potential denial of service or similar incident is notified and can be acted upon immediately. The Assurance Dashboard also takes feeds from anti-virus solutions so malware attacks can be identified and alerted on. If a major widespread cyber-attack were to happen (such as WANNACRY) the Assurance Dashboard would be updated to include a view identifying all devices on the network which have the exploited vulnerability. This then takes the identification task away from the Trust enabling them to move straight to remediation.

CAF Objective	CAF Indicator of Good Practice	How the Assurance Dashboard helps
C1.a Monitoring coverage *(continued)*	*Your monitoring data provides enough detail to reliably detect security incidents that could affect your essential service.*	The Assurance Dashboard provides granular detail of all IP addressable assets, ensuring that reliable monitoring and detection is carried out at all times.
C1.b Securing logs	*Access to logging data is limited to those with business need and no others.*	Access to the Assurance Dashboard is limited to those who have a business need to access the data. This can be further controlled by only giving those who need it full administration rights and read only access to others. The Assurance Dashboard also shows the privilege level of users to ensure that only those who need elevated privilege have these rights. This helps to control who has access to logging data.
C1.c Generating alerts	*Logging data is enriched with other network knowledge and data when investigating certain suspicious activity or alerts.*	The Assurance Dashboard collects a range of logging data related to devices and users and this can be used to support suspicious activity reporting.
	Alerts can be easily resolved to network assets using knowledge of networks and systems.	The Assurance Dashboard gives complete visibility of the network and network assets, therefore providing the information required to easily resolve alerts.
C1.d Identifying security incidents	*You have selected threat intelligence feeds using risk-based and threat-informed decisions based on your business needs and sector (e.g. vendor reporting and patching, strong anti-virus providers, sector and community-based infoshare).*	The Assurance Dashboard provides a number of threat intelligence feeds, including NHS Digital CareCERTs and WebChecker. In addition, it provides detailed information related to updates and patching from industry standard sources such as Microsoft (MSRC) Security Framework.
C1.e Monitoring tools and skills	*Your monitoring tools make use of all logging data collected to pinpoint activity within an incident.*	The Assurance Dashboard is able to provide visibility of logs collected from IP based devices and these are able to help identify incidents and related activity. In addition, the Assurance Dashboard will provide information from both endpoint devices and applications such as AV management consoles to support the DSP Toolkit.

C2. Proactive Security Event Discovery

Principle - *The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the delivery of essential services, even when the activity evades standard signature-based security prevent/detect solutions, or when it is not possible to use signature-based detection, for some reason.*

CAF Objective	CAF Indicator of Good Practice	How the Assurance Dashboard helps
C2.a System abnormalities for attack detection	*Normal system behaviour is fully understood to such an extent that searching for system abnormalities is a potentially effective way of detecting malicious activity. (e.g. You fully understand which systems should and should not communicate and when.*	The Assurance Dashboard gives visibility to the baseline posture for the organisation and any variations from this are notified, for example malicious behaviour or vulnerabilities. This allows the organisation to be fully aware at all times.

CAF Objective	CAF Indicator of Good Practice	How the Assurance Dashboard helps
C2.b Proactive attack discovery	*You have justified confidence in the effectiveness of your searches for system abnormalities indicative of malicious activity.*	The Assurance Dashboard is able to identify all devices on the network. Being dynamic in design, it provides the highest level of assurance and confidence without relying on third-party applications. The Assurance Dashboard interrogates the devices directly ensuring that all facets are covered including virus alerts, brute force attacks and unauthorised software installations. With all of the data fully drillable, Trusts can be very confident in the effectiveness of these searches.

D1. Response and Recovery Planning

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

CAF Objective	CAF Indicator of Good Practice	How the Assurance Dashboard helps
D1.a Generating alerts	*Your incident response plan is based on a clear understanding of the security risks to the networks and information systems supporting your essential service.*	The Assurance Dashboard gives Trusts a complete and dynamic picture of the network 24/7/365. It highlights vulnerable areas within the network and flags security gaps that require remediation. This information allows Trusts to develop an incident response plan that is based on a clear understanding of current security risks.

Increased visibility = Simplified compliance

For many NHS organisations, determining and proving compliance levels often means gathering the information required from across the estate, pulling it from a range of resources and disparate systems and then coordinating the reporting and matching it back to the requirements. It can be hugely time-consuming and place a great demand on resource. The compelling advantage of ITHealth's Assurance Dashboard Solution is that it pulls all facets of information into *one place* – ultimately increasing visibility of your network and providing a single and reliable source for what's happening within it – and it does so in near real-time. No more piecemealing of information or increased demands on resource. Only cost and time savings, less opportunity for error and a level of assurance you can trust.

Stay cyber assured and compliant

Call: 0115 987 6339

Email: info@ithealth.co.uk

Visit: www.ithealth.co.uk/assurance-dashboard

About ITHealth

ITHealth provide NHS organisations with proven and trusted IT security and access management solutions. Whether it's providing fast, reliable, and secure access for NHS mobile workers, or finding effective ways to reduce threats while improving productivity and clinical workflows, ITHealth's cost-effective solutions mean NHS systems and data are always secure, easy to access, and simple to manage.