FRAMEWORK CHECKLIST

Areas for growth

Dimension 1

□ I/My team have spoken to different staff members about their concerns with adopting cybersecurity measures and will address/have addressed the challenges raised, where possible

□ I/My team understand that ICT systems' maturity will partly influence the cybersecurity requirements of the organization and will consider/have considered the ICT used within my organization and what this will mean for cyber planning

□ I/My team understand that there are cultural factors and norms within the organization and in wider society that can undermine or promote cybersecurity and will/have considered what these factors and norms may be and how they can be encouraged (where they facilitate cybersecurity) or addressed (where they undermine cybersecurity)

□ I/My team have considered the main costs associated with scaling up cyber planning in my organization in the short-term (e.g., 1 year) and long-term (e.g., 5-10 years) and will/have discussed these needs with relevant finance/leadership stakeholders in my organization

Dimension 2

□ I/My team have considered the value and appropriate content of an incident communication plan and will/have developed a communication plan as part of wider incident response planning

□ I/My team have considered the value of and appropriate content for communicating threats to stakeholders and will/have developed a plan to regularly communicate threats to different stakeholders in the organization

□ I/My team have reviewed which national and international frameworks and regulations are mandatory for my healthcare organization to implement and follow, and have created/will create a matrix showing which controls and certifications should be implemented or strengthened to safely continue operations

□ I/My team understand the use of health/clinical information standards and documented/will document where standards may be applied and secured based on the various connections within my organization

□ I/My team understand the importance of a clinical safety assessment process and the means of supporting clinical safety and have developed/will develop a clinical safety assessment process

□ I/My team understand the concepts of WFH and BYOD and their potential impact on organizational cybersecurity and have developed/will develop policies to minimize and mitigate risks

□ I/My team understand the value of developing positive organizational memory and have developed/will develop a plan for capturing or adopting best practice in key cybersecurity areas, engaging the organization to find and spread locally developed best practice

□ I/My team understand the threat of cyber-attacks on medical devices and have mapped/will map all medical devices, including those without internet connectivity, and have assessed/will assess these for cyber-risks backed by a plan to remediate any such risks

□ I/My team have created or adopted/will create or adopt practices for regular system and device testing to expose any vulnerabilities and mitigate risks

□ I/My team have mapped/will map services and protocols across networks and have adopted/will adopt a policy that minimises any unnecessary communication

Dimension 3

□ I/My team understand the value of a business continuity plan and have developed/are in the process of developing a BCP, including data backups and tested this for critical systems and applications, as well as the ability to restore from backup

□ I/My team have developed/are in the process of developing a basic cybersecurity strategy supported by a list of elements requiring cybersecurity and a RACI matrix attached to those elements

□ I/My team have estimated a required budget for cybersecurity based on my healthcare organization's needs, year-on-year for the next three years, and have presented/will present this to the board

□ I/My team understand the value of a communications strategy related to communications and have created/will create and adopt a cybersecurity communications plan that also includes or references an IRP

□ I/My team have considered how the board can be engaged on cybersecurity and preparedness planning across the organization and will/have discussed including cybersecurity as a regular item on the agenda of meetings with the board

□ I/My team understand the added value a Security Steering Group can add to cyber preparedness planning in my organization and, if considered a valuable resource, will/have set up a Steering Group

□ I/My team have assessed security requirements for procurement and applied this to procurement processes and third-party suppliers

Dimension 4

- □ I/My team have adopted or created or are working towards an annual cyber risk assessment and understand how to apply this to our people and technology
- □ I/My team are aware of the risk posed by phishing emails and have developed/will develop relevant technical controls in place to support staff. The team has also planned/will plan specific phishing awareness in to the wider cyber awareness programme planning
- □ I/My team have created a minimum information asset register and are in the process of assigning unique asset identifiers to every organizational asset
- □ I/My team have completed an initial network and data flow map and plan to continue improving these maps through regular review
- □ I/My team have assessed our supply chains and determined single points of failure and/or weak security standards
- □ I/My team have embedded/will embed cyber risk into the healthcare organization's existing risk process, or in cases where this is not possible have developed/will develop an organizational risk matrix and change management risk classification system
- □ I/My team have developed or are in the process of developing a framework for root cause analysis and lessons learned and are applying/will apply this to any suspected or actual nonconformance going forward
- □ I/My team have developed or are in the process of developing a policy and schedule for internal and external audits
- □ I/My team have considered our needs for monitoring, logging, and alerting and have developed/will develop a policy for how to utilize these tools, what to log, and for how long
- □ I/My team understand the importance of developing emergency processes and have developed/will develop an incident response plan as part of our organizational strategy outputs
- □ I/My team understand what is meant by internal risk management and examples of actions and policies that can be put in place to mitigate risk
- □ I/My team have understand what is meant by external risk management and examples of actions and policies that can be put in place to mitigate risk
- □ I/My team have developed a set of simulation attacks along with response plans with the intention to test readiness on an annual basis at a minimum
- □ I/My team understand that suppliers and partners are held to the same high security standards as our healthcare organization and have reviewed/will review third-party supplier contracts to assess requirements for external audit

Dimension 5

□ I/My team have considered the importance in engaging ALL staff on cybersecurity and will/have developed awareness raising and engagement activities and resources

□ I/My team have developed a matrix that outlines cyber-security vetting requirements for every job description and have reviewed the matrix with HR and hiring managers

□ I/My team have developed, adopted, or purchased appropriate training courses for cybersecurity and data protection and aligned this with our regularly updated cybersecurity matrix for job descriptions

□ I/My team have considered the scope and deployment of materials and resources outlining cybersecurity regulations, best practices, and reporting systems in place and will/have developed and deployed these materials

Dimension 6

□ I/My team have considered how and to whom access is granted and how that access is monitored and will consider/address improvements where possible

□ I/My team have created an access management policy, including password policy, that reflects the need for identity management, identity validation, and application tokens

□ I/My team have created an acceptable use policy for personal devices/software and an update policy for connected devices to ensure software and firmware are up to date

□ I/My team have investigated the use of anomaly detection software for monitoring threats and have drafted a monitoring policy for systems

□ I/My team have developed a patching and software update policy backed by a catalog of known technology assets that require updating

□ I/My team have created a policy to describe where our organization requires encryption both at rest and in transit

□ I/My team have examined and described organizational applications and services in a way which allows the organization to reduce unwarranted trust and communication between systems

□ I/My team have developed a policy for installation of appropriate antimalware and antivirus software and have considered additional points of entry for malicious software into the organization

□ I/My team have reviewed the use cases for data usage and will write/have written a policy for minimization that supports purpose-based data releases

□ I/My team have created/are working towards creating a checklist with minimum hardware, software, and standards for technology procurement or development for our organization

□ I/My team have developed a policy for internet access, considering the full spectrum of user requirements and potential consequences of intended access controls

□ I/My team have reviewed our need for on-premises services against benefits of migrating to cloud and developed/will develop a list of cloud migration candidates