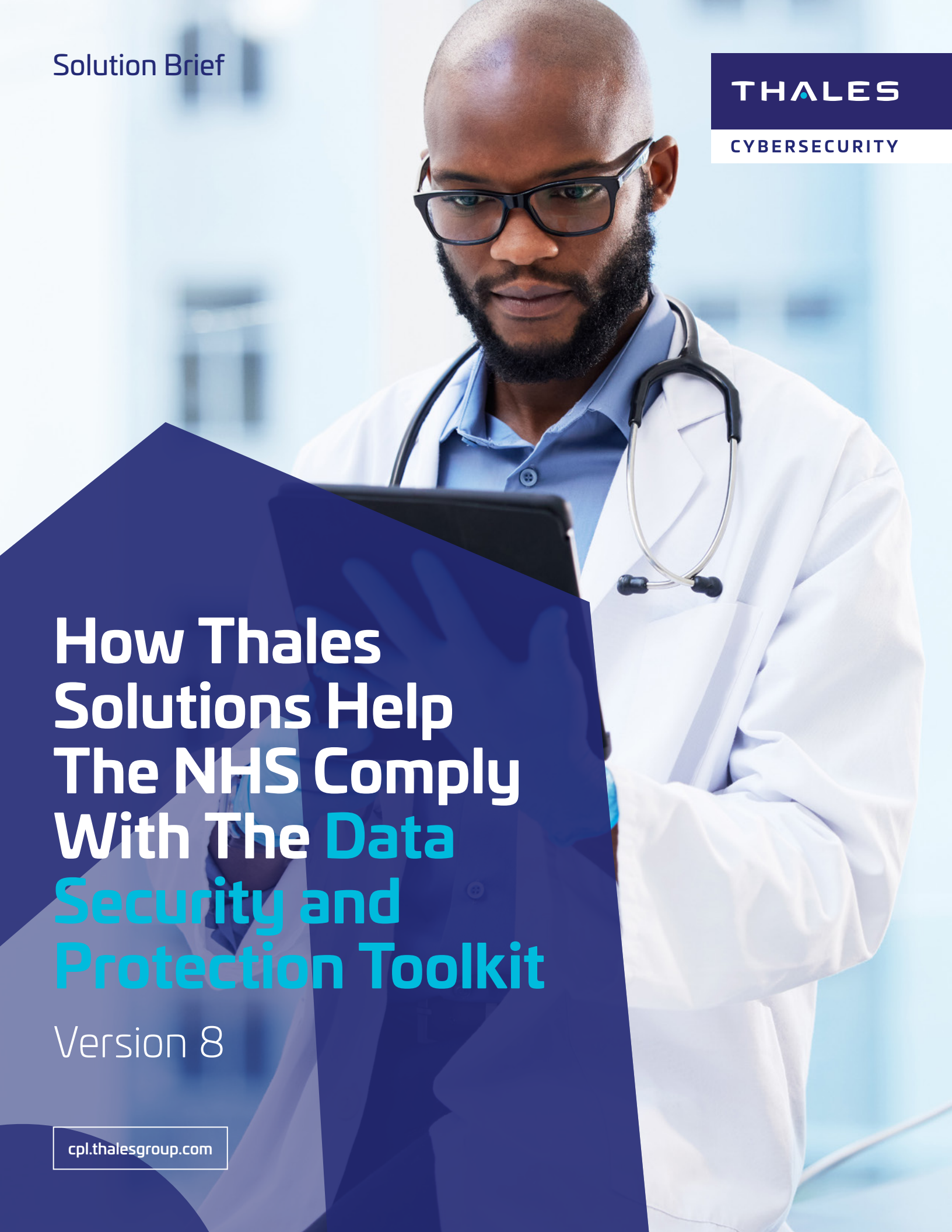
Solution Brief

THALES

CYBERSECURITY



How Thales Solutions Help The NHS Comply With The Data Security and Protection Toolkit

Version 8

cpl.thalesgroup.com

THALES

CYBERSECURITY

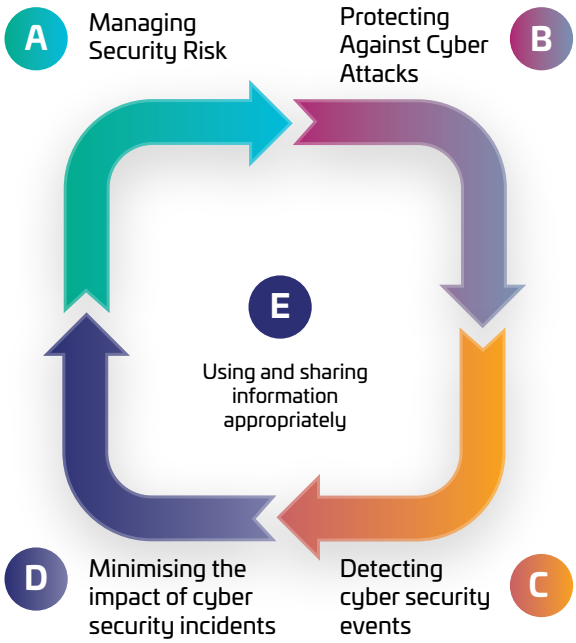
What is the Data Security and Protection Tookit?:

The Data Security and Protection Toolkit (DSPT) is an online self-assessment tool designed to help NHS organisations measure and demonstrate their compliance with data protection and information security requirements. By completing the toolkit, National Health organisations can systematically evaluate their policies, processes, and technical measures, identify any areas of improvement, and provide assurance to stakeholders that appropriate data protection controls are in place.

Important Dates for DSPT v8:

The deadline for the self-assessment on the Data Security and Protection Toolkit v8 is 30th June 2026.

Thales helps NHS organisations through the self-assessment through managing security risk, protecting against cyber attacks, detecting cyber security events and minimizing the impact of cyber security incidents.



Function	Category	Thales Capabilities
Govern (GV)	• **Organizational Context** • **Risk Management Strategy** • **Cybersecurity Supply Chain Risk Management** • **Roles, Responsibilities, and Authorities** • **Oversight**	• Gain visibility, control, and insight over sensitive data and compliance status. • Produce uniform data risk status and risk score by consolidating data risk metrics. • Prioritize risk mitigation with clear recommendations for corrective action. • Reduce third party risk by protecting apps, data and identities in the cloud. • Enforce security policy and regulatory requirements over data, access and identities.
Identify (ID)	• **Asset Management** • **Risk Assessment** • **Improvement**	• Find and classify sensitive data based on regulatory requirements. • Use machine learning to improve risk detection and scoring. • Inspect incoming requests to applications, identify malicious activity, and block attacks.
Protect (PR)	• **Identity Management, Authentication, and Access Control** • **Awareness and Training** • **Data Security** • **Platform Security** • **Technology Infrastructure Resilience**	• Protect access and identities with MFA and adaptive contextual policies. • Centralize access control over multiple hybrid environments in a single pane of glass • Protect data at rest, in motion, and in use with FIPS 140-2 level encryption. • Monitor data usage and enforce policy across hybrid IT. • Continuously monitor cyber traffic, detect and prevent cyber threats to applications. • Mitigate DDoS attacks in as little as three seconds, prevent malicious Bot attacks.
Detect (DE)	• **Continuous Monitoring** • **Adverse Event Analysis**	• Monitor API usage, detect anomalies, detect and prevent web-based attacks. • Produce audit trail and reports of all access events to all systems, stream logs to SIEM. • Forensics investigations on all observed activity provide insight into events.
Respond (RS)	• **Incident Management** • **Incident Analysis** • **Incident Response Reports and Communication** • **Incident Mitigation**	• Mitigate DDoS attacks within 3 seconds or less with no impact to performance. • Monitor for abnormal I/O activity and block malware before it takes hold. • Leverage automation and machine learning to block malicious traffic at the edge. • Playbooks perform various tasks, such as responding to outliers, anomalies, and threats.
Recover (RC)	• **Incident Recovery Plan Execution** • **Incident Recovery Communication**	• Create detailed reports for audits and reporting. • Leverage automated workflows within CMDB and SOAR to start restoring and recovering

Description	ISO/IEC 27001:2022 Parallels	Thales Solutions
Managing Risk Asset management		
A3 (A3.a) Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).	**5.12: Classification of Information:** Information should be classified according to the information security needs.	**CipherTrust Data Discovery and Classification** identifies structured and unstructured sensitive data on-premises and in the cloud. Built-in templates enable rapid identification of regulated data, highlight security risks, and help uncover compliance gaps.
Managing Risk Supply chain		
A4 (A4.a) The organisation understands and manages security and IG risks to information, systems and networks supporting the operation of essential functions that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.	**5.23: Information security** for use of cloud services Processes for acquisition, use, management, and exit from cloud services should be established.	**CipherTrust Cloud Key Manager** can reduce third cloud security risks by maintaining on-premises under the full control of the organization the keys that protect sensitive data hosted by third party cloud providers under "bring your own keys" (BYOK) systems. **CipherTrust Transparent Encryption** provides complete separation of administrative roles, where only authorized users and processes can view unencrypted data. Unless a valid reason to access the data is provided, sensitive data stored in a third-party cloud will not be accessible in cleartext to unauthorized users.
Procedures and Policies Protecting against cyber-attack and data breaches		
B1 (B1.a) You have developed and continue to improve a set of information assurance and resilience policies, processes and procedures that manage and mitigate the risk of adverse impact on your essential function.	**5.15: Access Control Rules** to control physical and logical access to information and other associated assets should be established and implemented **5.17: Authentication information** Allocation and management of authentication information should be controlled by a management process. **5.18: Access Rights** Access rights to information should be provisioned, reviewed, modified, and removed according to policy. **5.34: Privacy and Protection** of PII Identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements. **8.24: Use of Cryptography Rules** for the effective use of cryptography, including cryptographic key management, should be defined and implemented **8.25: Secure development lifecycle Rules** for the secure development of software and systems should be established and applied.	**Thales OneWelcome** identity and access management solutions limit the access of internal and external users based on their roles and context. Backed by strong authentication (MFA), granular access policies and fine-grained authorization policies help ensure the right user is granted access to the right resource at the right time. This minimizes the risk of unauthorized access. **CipherTrust Data Security Platform** is an integrated suite of data-centric security products and solutions that unify data discovery, protection, and control in one platform. CipherTrust Platform provides multiple capabilities for protecting data at rest in files, volumes, and databases. **Thales Luna Hardware Security Modules (HSMs)** protect cryptographic keys and provide a FIPS 140-2 Level 3 hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption, and more. Luna HSMs are available on-premises, in the cloud as-a-service, and across hybrid environments. **CipherTrust Application Data Protection** offers developer-friendly software tools for encryption key management as well as application-level encryption of sensitive data. It can take place immediately upon data creation or first processing and can remain encrypted regardless of its data life cycle state – during transfer, use, backup or copy, to provide the highest level of security at the application layer.

Description	ISO/IEC 27001:2022 Parallels	Thales Solutions
Procedures and Policies Protecting against cyber-attack and data breaches		
B1 (B1.b) You have successfully implemented your information assurance policies, processes and procedures and can demonstrate the benefits achieved.	**5.15: Access Control Rules** to control physical and logical access to information and other associated assets should be established and implemented. **8.3: Information Access Restriction** Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control. **8.24: Use of Cryptography Rules** for the effective use of cryptography, including cryptographic key management, should be defined and implemented **8.25: Secure development lifecycle Rules** for the secure development of software and systems should be established and applied.	**Thales OneWelcome Consent & Preference Management** module enables organizations to gather the consent of end consumers, so, for example, financial institutions have clear visibility of consented data allowing them to manage access to data they are allowed to utilize. **CipherTrust Transparent Encryption** encrypts sensitive data and enforces granular privileged-user-access management policies that can be applied by user, process, file type, time of day, and other parameters. It provides complete separation of roles, where only authorized users and processes can view unencrypted data. **CipherTrust Platform Community Edition** makes it easy for DevSecOps to deploy data protection controls in hybrid and multi-cloud applications. The solution includes licenses for CipherTrust Manager Community Edition, Data Protection Gateway, and CipherTrust Transparent Encryption for Kubernetes.
B2 (B2.a) You robustly verify, authenticate and authorise access to the information, systems and networks supporting your essential function(s).	**5.17: Authentication information** Allocation and management of authentication information should be controlled by a management process. **6.7: Remote Working Security** measures should be implemented when personnel are working remotely. **8.5: Secure Authentication** Secure authentication technologies and procedures should be implemented.	**Thales OneWelcome** identity and access management solutions limit the access of internal and external users based on their roles and context. Backed by strong authentication (MFA), granular access policies and fine-grained authorization policies help ensure the right user is granted access to the right resource at the right time. This minimizes the risk of unauthorized access. **SafeNet Trusted Access** is a cloud-based access management solution that provides commercial, off-the-shelf multi-factor authentication with the broadest range of hardware and software authentication methods and form factors. **Thales converged badge** solutions simplify the management of physical and logical access by consolidating all corporate security applications in a single user's badge: physical access to buildings and restricted areas, visual identification of the cardholder, secure access to sensitive digital resources thanks to PKI-certificate based and/ or FIDO authentication.
B2 (B2.c) You closely manage privileged user access to networks and information systems supporting your essential function(s).	**5.3: Segregation of Duties** Conflicting duties and conflicting areas of responsibility should be segregated.	**CipherTrust Transparent Encryption** delivers data-at-rest encryption with centralized key management and privileged user access control. It provides a complete separation of roles, where only authorized users and processes can view unencrypted data. This ensures privacy and protects sensitive data wherever it resides, on-premises, across multiple clouds, and within big data and container environments.
B2 (B2.d) You closely manage and maintain identity and access control for users, devices and systems accessing the network and information systems supporting your essential function(s).	**5.15: Access Control Rules** to control physical and logical access to information and other associated assets should be established and implemented. **5.18: Access Rights** Access rights to information should be provisioned, reviewed, modified, and removed according to policy. **8.3: Information Access Restriction** Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.	**Thales OneWelcome** identity and access management solutions limit the access of internal and external users based on their roles and context. Backed by strong authentication (MFA), granular access policies and fine-grained authorization policies help ensure the right user is granted access to the right resource at the right time. This minimizes the risk of unauthorized access. **SafeNet Trusted Access** is a cloud-based access management solution that provides commercial, off-the-shelf multi-factor authentication with the broadest range of hardware and software authentication methods and form factors. **CipherTrust Transparent Encryption** encrypts sensitive data and enforces granular privileged-user-access management policies that can be applied by user, process, file type, time of day, and other parameters. It provides complete separation of roles, where only authorized users and processes can view unencrypted data.

Description	ISO/IEC 27001:2022 Parallels	Thales Solutions
Procedures and Policies Protecting against cyber-attack and data breaches		
B3 (B3.a) You have a good understanding of data important to the operation of your essential function(s), where it is stored, where it travels and how unavailability or unauthorised access, modification or deletion would adversely impact the essential function(s). This also applies to third parties storing or accessing data important to the operation of your essential function(s).	8.10: Information Deletion Information stored in information systems, devices or in any other storage media should be deleted when no longer required.	**CipherTrust Data Security Platform** is an integrated suite of data-centric security products and solutions that unify data discovery, protection, and control in one platform. CipherTrust Platform provides multiple capabilities for protecting data at rest in files, volumes, and databases
B3 (B3.b) You have protected the transit of data important to the operation of your essential function(s). This includes the transfer of data to third parties.	8.12: Data Leakage Prevention Data leakage prevention measures should be applied to systems, networks, and any other devices that process, store, or transmit sensitive information. 8.24: Use of Cryptography Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented	**Thales Luna Hardware Security Modules (HSMs)** protect cryptographic keys and provide a FIPS 140-2 Level 3 hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption, and more. Luna HSMs are available on-premises, in the cloud as-a-service, and across hybrid environments. Luna HSMs: • Generate and protect root and certificate authority (CA) keys, providing support for PKIs across a variety of use cases • Sign application code to ensure software remains secure, unaltered, and authentic. • Create digital certificates for credentialing and authenticating proprietary electronic devices for IoT applications and other network deployments. **Thales High Speed Encryptors (HSEs)** provide network-independent data-in-motion encryption (layers 2, 3, and 4) ensuring data is secure as it moves from site-to-site, or from on-premises to the cloud and back. Our network encryption solutions allow customers to limit data leaks and better protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception— without performance compromise.
B3 (B3.c) You have protected stored soft and hard copy data important to the operation of your essential function(s).	**5.33: Protection of Records** Records should be protected from loss, destruction, falsification, unauthorized access, and unauthorized release **5.34: Privacy and Protection of PII** Identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements. **6.7: Remote Working** Security measures should be implemented when personnel are working remotely. **8.4: Access to Source Code** Read and write access to source code, development tools, and software libraries should be managed. **8.12: Data Leakage Prevention** Data leakage prevention measures should be applied to systems, networks, and any other devices that process, store, or transmit sensitive information.	**CipherTrust Transparent Encryption** delivers data-at-rest encryption with centralized key management and privileged user access control. It provides a complete separation of roles, where only authorized users and processes can view unencrypted data. This ensures privacy and protects sensitive data wherever it resides, on-premises, across multiple clouds, and within big data and container environments. **CipherTrust Tokenization** with dynamic data masking permits the pseudonymization of sensitive information in databases while maintaining the ability to analyze aggregate data without exposing sensitive data during the analysis or in reports. Thales converged badge solutions simplify the management of physical and logical access by consolidating all corporate security applications in a single user's badge: physical access to buildings and restricted areas, visual identification of the cardholder, secure access to sensitive digital resources thanks to PKI-certificate based and/ or FIDO authentication. **CipherTrust Transparent Encryption Ransomware Protection (CTE-RWP)** continuously monitors processes for abnormal I/O activity and alerts or blocks malicious activity before ransomware can take complete hold of your endpoints and servers. It monitors active processes to detect ransomware – identifying activities such as excessive data access, exfiltration, unauthorized encryption, or malicious impersonation of a user, and alerts/blocks when such an activity is detected.

Description	ISO/IEC 27001:2022 Parallels	Thales Solutions
Procedures and Policies Protecting against cyber-attack and data breaches		
B4 (B4.a) You design security into the network and information systems that support the operation of your essential function(s). You minimise their attack surface and ensure that the operation of your essential function(s) should not be impacted by the exploitation of any single vulnerability.	**6.7: Remote Working** Security measures should be implemented when personnel are working remotely.	**SafeNet Trusted Access** is a cloud-based access management solution that provides commercial, off-the-shelf multi-factor authentication with the broadest range of hardware and software authentication methods and form factors.
B4 (B4.c) You manage your organisation's network and information systems that support the operation of your essential function(s) to enable and maintain security.	**8.7: Protection against Malware** Protection against malware should be implemented and supported by appropriate user awareness	**CipherTrust Data Security Platform** is an integrated suite of data-centric security products and solutions that unify data discovery, protection, and control in one platform. CipherTrust Platform provides multiple capabilities for protecting data at rest in files, volumes, and databases.
B5 (B5.b) You design the network and information systems supporting your essential function(s) to be resilient to cyber security incidents. Systems are appropriately segregated and resource limitations are mitigated.	**8.14 Information processing facilities** should be implemented with redundancy sufficient to meet availability **8.23 Access to external websites** should be managed to reduce exposure to malicious content	**Thales Luna HSM** partitions can be configured in high-availability groups for redundancy and reliability. Luna HSMs can provide scalability and redundancy for cryptographic applications that are critical to your organization. For applications that require continuous, uninterruptible uptime, the Luna HSM Client allows you to combine application partitions on multiple HSMs into a single logical group, known as a High-Availability (HA) group. **Imperva's Web Application Firewall (WAF)** provides out-of-the-box security for your web applications. It detects and prevents cyber threats, ensuring seamless operations and peace of mind. Protect your digital assets with Imperva's robust, industry-leading solution.
B6 (B6.b) The people who support the operation of your essential function(s) are appropriately trained in information assurance. A range of approaches to information assurance training, awareness and communications are employed.	**5.17: Authentication information** Allocation and management of authentication information should be controlled by a management process." **8.7: Protection against Malware** Protection against malware should be implemented and supported by appropriate user awareness	**Thales OneWelcome** identity and access management solutions limit the access of internal and external users based on their roles and context. Backed by strong authentication (MFA), granular access policies and fine-grained authorization policies help ensure the right user is granted access to the right resource at the right time. This minimizes the risk of unauthorized access. **CipherTrust Data Security Platform** is an integrated suite of data-centric security products and solutions that unify data discovery, protection, and control in one platform. CipherTrust Platform provides multiple capabilities for protecting data at rest in files, volumes, and databases.

Description	ISO/IEC 27001:2022 Parallels	Thales Solutions
Detecting Cyber Security Events Capabilities exist to minimise the adverse impact of an incident on the operation of essential functions, including the restoration of those functions where necessary, and to uphold the rights of impacted individuals.		
C1 (C1.a) The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function(s).	**8.7: Protection against Malware** Protection against malware should be implemented and supported by appropriate user awareness	**CipherTrust Data Security Platform** is an integrated suite of data-centric security products and solutions that unify data discovery, protection, and control in one platform. CipherTrust Platform provides multiple capabilities for protecting data at rest in files, volumes, and databases. **Thales Data Security** solutions offer the most comprehensive range of data protection, such as Thales Data Protection on Demand (DPoD) that provides built in high availability and backup to its cloud-based Luna Cloud HSM and CipherTrust Key Management services
D1 (D1.a) You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of your essential function(s) and covers a range of incident scenarios.	**5.30: ICT readiness for business continuity** ICT readiness should be planned, implemented, maintained, and tested based on business continuity objectives	
Using and sharing information appropriately The organisation ensures that information is used and shared lawfully and appropriately.		
E4 (E4.a) The organisation manages records in accordance with its professional responsibilities and the law.	**5.33: Protection of Records** Records should be protected from loss, destruction, falsification, unauthorized access, and unauthorized release	**CipherTrust Data Security Platform** is an integrated suite of data-centric security products and solutions that unify data discovery, protection, and control in one platform. **CipherTrust Platform** provides multiple capabilities for protecting data at rest in files, volumes, and databases.
	5.34: Privacy and Protection of PII Identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	