GuardWare INSIGHT helps organisations conform to NIST 800-171, Revision 2

HELPS TO CONFORM TO NIST SP 800-171, REVISION 2

What is Controlled Unclassified Information (CUI)?

Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies.

What is NIST 800-171, Revision 2?

As computing platforms and technologies are ubiquitously deployed worldwide and systems and components are increasingly interconnected through wired and wireless networks, the susceptibility of Controlled Unclassified Information (CUI) to loss or compromise grows.

The purpose of NIST SP 800-171 is to provide federal agencies with recommended security requirements for protecting the confidentiality of CUI, when the CUI is resident in a non-federal information system and with organizations such as contractors.

Who needs to follow NIST SP 800-171, Revision 2?

The standard is applicable to any prime contractor or sub-contractor who works on government projects, where it is highly likely they have access to CUI. Such organisations need to implement the necessary controls as per this standard.

What is GuardWare INSIGHT?

GuardWare INSIGHT is an information security solution that helps companies monitor and secure sensitive information such as CUI. The following are some of the key capabilities of this solution:

1. Discovers and classifies sensitive information from various sources including ERPs, databases and file-stores.
2. Provides data breach monitoring and alerting. Monitors the access, deletion, modification and movement of sensitive data (files and text) on all corporate and non-corporate channels and alerts if data breach occurs.
3. Pre-empt issues by monitoring possible malicious changes in user behaviour using advanced behaviour analytics and machine learning.
4. Automates risk and security assessment processes.
5. Monitors the organisational environment using configuration management features such as software auditing and highlights issues such as the use of malicious programs or out-of-date PC configurations.

How can GuardWare INSIGHT help companies comply with NIST SP 800-171, Revision 2?

Below is the summary table showcasing INSIGHT applicability. The summary table is followed by detailed break down and mapping of GuardWare INIGHT to NIST SP 800-171 Rev 2 security requirements.

- Green Colour depicts most technical major technical controls are addressed.
- Orange colour depicts partial technical controls are addressed.

NIST SP 800-171 Security Families	GuardWare INSIGHT Applicability
Access Control	Partial Coverage
Awareness and Training	Most Technical Requirements Covered
Audit and Accountability	Most Technical Requirements Covered
Configuration Management	Most Technical Requirements Covered
Identification and Authentication	Partial Coverage
Incident response	Most Technical Requirements Covered
Maintenance	Partial Coverage
Media Protection	Most Technical Requirements Covered
Personnel Security	Most Technical Requirements Covered
Physical Protection	Not Covered
Risk Assessment	Most Technical Requirements Covered
Security Assessment	Most Technical Requirements Covered
System and Communications Protection	Partial Coverage
System and Information Integrity	Partial Coverage

Detailed Mapping of NIST SP 800-171 Revision to GuardWare INSIGHT

- Yellow colour depicts basic security requirements of the security family.
- Green Colour depicts most technical major technical controls are addressed
- Orange colour depicts partial technical controls are addressed.

Family	Basic/Derived Security Requirement	Identifier	Security Requirement	GuardWare INSIGHT Applicability
Access Control	Basic	3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	• Facilitates the application of access control policies on sensitive information. • Provides a complete and non-repudiable audit trail. Information owners and IT security receive alerts and can review actions in the case of unauthorised access.
Access Control	Basic	3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	
Access Control	Derived	3.1.3	Control the flow of CUI in accordance with approved authorizations.	Allows for specific monitoring and control of CUI data. Movement and usage of CUI data can be blocked or alerted upon when emailed, copied to USB, printed or uploaded to Web.
Access Control	Derived	3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	INSIGHT helps to decentralise information monitoring and control. The system offers several roles with the goal of separating duties among IT, IT Sec, Information Owners and Top Management.
Access Control	Derived	3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	The system helps to enforce the principal of least privilege by monitoring all non-security and privileged actions performed by the users. The system alerts if there is inconsistency in functions performed by the user and their associated role. The system also applies the principal of least privilege in the configuration and monitoring control. The system support several roles and division of functions among those roles.
Access Control	Derived	3.1.6	Use non-privileged accounts or roles when	Monitors all actions of users and alerts if privileged functions are performed by non-privileged accounts.

			accessing nonsecurity functions	
Access Control	Derived	3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Monitors execution of privileged functions by users and reports about the event.
Access Control	Derived	3.1.8	Limit unsuccessful logon attempts.	
Access Control	Derived	3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	Alerts on the access and usage of CUI information. Alerts can be customised to specific CUI information.
Access Control	Derived	3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity	
Access Control	Derived	3.1.11	Terminate (automatically) a user session after a defined condition.	Supports logging off, hibernating of devices if not in use
Access Control	Derived	3.1.12	Monitor and control remote access sessions.	Monitors and controls the use of remote sessions established via VPN applications or Web.
Access Control	Derived	3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	
Access Control	Derived	3.1.14	Route remote access via managed access control points.	
Access Control	Derived	3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	

Access Control	Derived	3.1.16	Authorize wireless access prior to allowing such connections	Reports on the usage of wireless connections. Alerts on the use unsanctioned wireless connections.
Access Control	Derived	3.1.17	Protect wireless access using authentication and encryption	Reports on the usage of wireless connections. Alerts on the use unsanctioned wireless connections.
Access Control	Derived	3.1.18	Control connection of mobile devices.	Reports on connections used by Mobile Devices. Ability to whitelist connections to be used.
Access Control	Derived	3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.[23]	
Access Control	Derived	3.1.20	Verify and control/limit connections to and use of external systems.	Monitors access of external online systems. Allows for granular control over who can and cannot access external systems. Allows for block, alert or silently monitor and report capabilities on access of remote external systems.
Access Control	Derived	3.1.21	Limit use of portable storage devices on external systems.	Monitors and controls the use of external storage devices. The control can be specific to particular user, device and type of information like CUI. The system also alerts on the usage of non-corporate, unencrypted external storage devices.
Access Control	Derived	3.1.22	Control CUI posted or processed on publicly accessible systems.	GuardWare INSIGHT monitors and controls all forms of offline and online communication channels. Monitoring and Control can focused on specific CUI information. These include: o Any corporate sources like emails, teams, data sharing apps and SharePoint. o Offline sources like USBs, Bluetooth, print and phone sync. o Any non-corporate encrypted channels like free emails, cloud, websites, chat including WhatsApp, WeChat and Telegram.
Awareness and Training	Basic	3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures	INSIGHT helps to facilitate the requirement of security risk awareness among company staff. • GuardWare INSIGHT assists in the implementation of the Trusted Insider Programme as required under DISP. It implements the Trusted Insider controls as per the ACSC ISM. • GuardWare INSIGHT's user behaviour analytics capabilities help to raise awareness among staff about the importance of securing sensitive information. This is done by monitoring their behaviour and producing

			related to the security of those systems.	alerts when they perform risky actions such as syncing CUI to personal mobile phone or sending it to the wrong person. The reports are sent not only to IT but also to the department heads, who can assist in raising awareness about the risky actions performed by their staff. • The detected incidents are used by company's IT security teams to educate the users about where they have gone wrong, raise their awareness towards cyber security, and in the case of malicious activity take disciplinary actions.
Awareness and Training	Basic	3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
Awareness and Training	Derived	3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	
Audit and Accountability	Basic	3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity	Maintains complete Audit log of all user and admin actions. This includes system access and changes made. Logs cannot be deleted. The system also has the ability to alert in case it is tempered with. Further system has built in anti-tempering features which prevent privileged users from deleting, modifying, changing and deleting any of the system services and logs.

Audit and Accountability	Basic	3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.	Provides a complete and non-repudiable audit trail. Information owners and IT security receive alerts and can review actions in the case of risky an unauthorised activities. All monitoring is done from a user's point of view. Hence it facilitates an investigation. The following information is available regarding each transgression: o User involved. o Information involved down to content level. o Device involved. o Date and time. o Exfiltration method used such as copying to USB, printing, etc. o Visual evidence in the form of screenshots. o Network or communication channel used. o User's action before and after the transgression. o Behaviour trends of the user.
Audit and Accountability	Derived	3.3.3	Review and update logged events.	Provide several means of reviewing and analysing logs. This includes Dashboard, email and excel based analysis tools.
Audit and Accountability	Derived	3.3.4	Alert in the event of an audit logging process failure.	Alerts if logging fails
Audit and Accountability	Derived	3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	Provide several means of reviewing and analysing logs. This includes Dashboard, email based alerting, risk based reporting, Artificial Intelligence based reports and excel based analysis tools. Reports can be generated on demand basis based on specific conditions and scenarios required for investigation.
Audit and Accountability	Derived	3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.	
Audit and Accountability	Derived	3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to	GuardWare Cloud servers are synchronised by AWS. All reports coming from end-point carry the end user time stamp and can be correlated back with the server. This establishes when the actual event happened and when it was reported.

			generate time stamps for audit records	
Audit and Accountability	Derived	3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	Logs cannot be deleted. The system also has the ability to alert in case it is tempered with. Further system has built in anti-tempering features which prevent privileged users from deleting, modifying, changing and deleting any of the system services and logs.
Audit and Accountability	Derived	3.3.9	Limit management of audit logging functionality to a subset of privileged users.	The system supports multiple roles. Different users based on their roles can be given access to specific logs. Logs can be divided based on user groups and type of log data.
Configuration Management	Basic	3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	• GuardWare INSIGHT's offers hardware, software and network audit modules as part of the one-stop solution. These modules help to baseline the hardware and software configurations of a company's network and to report any unauthorised changes. For example, the software audit module highlights any unauthorised software installed in the devices or any non-standard configuration of installed software. • INSIGHT blocks (blacklisting) use of unauthorised applications whether desktop or online variants. • INSIGHT blocks (blacklisting) use of unauthorised network connections. These include wired and wireless connections. • The requirement also relates to data. In that aspect GuardWare INSIGHT maintains a real-time full inventory of the location and usage of marked CUI documents within any given period. This includes documents maintained in network stores, PCs, and mobile devices. • Helps in taking an inventory of the digital assets by performing data discovery scans to locate where sensitive data is stored. • Automatically classifies sensitive data which includes the requirements of handling Defence Information. • Ensures proper use of sensitive assets by monitoring their access, usage, transfer, and storage.
Configuration Management	Basic	3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.	
Configuration Management	Derived	3.4.3	Track, review, approve or disapprove, and log changes to organizational systems.	
Configuration Management	Derived	3.4.4	Analyze the security impact of changes prior to implementation.	

Configuration Management	Derived	3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	
Configuration Management	Derived	3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	
Configuration Management	Derived	3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	• INSIGHT blocks (blacklisting) use of unauthorised applications whether desktop or online variants. • INSIGHT blocks (blacklisting) use of unauthorised network connections. These include wired and wireless connections. • Monitors usage of all online and desktop based installed software
Configuration Management	Derived	3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	
Configuration Management	Derived	3.4.9	Control and monitor user-installed software.	

Identification and Authentication	Basic	3.5.1	Identify system users, processes acting on behalf of users, and devices.	GuardWare INSIGHT partially fulfils this requirement, as it is largely to do with having an appropriate identity and access management system and password management system in place. Following is how INSIGHT assists: • Facilitates the application of access control policies on sensitive information. • Provides a complete and non-repudiable audit trail. Information owners and IT security receive alerts and can review actions in the case of unauthorised access. • Helps to ensure defence classified data and ITAR related information is being accessed by authorised users.
Identification and Authentication	Basic	3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	
Identification and Authentication	Derived	3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.[24] [25].	
Identification and Authentication	Derived	3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	
Identification and Authentication	Derived	3.5.5	Prevent reuse of identifiers for a defined period.	
Identification and Authentication	Derived	3.5.6	Disable identifiers after a defined period of inactivity.	

Identification and Authentication	Derived	3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	
Identification and Authentication	Derived	3.5.8	Prohibit password reuse for a specified number of generations.	
Identification and Authentication	Derived	3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	
Identification and Authentication	Derived	3.5.10	Store and transmit only cryptographically-protected passwords.	
Identification and Authentication	Derived	3.5.11	Obscure feedback of authentication information	
Incident response	Basic	3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	GuardWare INSIGHT offers complete incident response capabilities. • The system provides workflow management for reported incidents. Incidents can be routed (based on their type) to relevant information owners, CSOs or TCO (Technology Control Officers) in case of ITAR. The system provides excel based reporting to information owners for ease of use. Information owners are provided with access accounts to the system and to the relevant incidents. They can review the incidents and decide if they require further action or should be closed, by selecting the appropriate option in the system.

Incident response	Basic	3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	• The detected incidents are used by company's IT security teams to educate the users about where they have gone wrong, raise their awareness towards cyber security, and in the case of malicious activity take disciplinary actions. • The system generates overall incident reports for management review. This ensures that all involved parties are performing their jobs.
Incident response	Derived	3.6.3	Test the organizational incident response capability.	The system is central to the incident response capability. It provides the mechanism by which organisations can simulate and test out how they will handle a particular response.
Maintenance	Basic	3.7.1	Perform maintenance on organizational systems.	
Maintenance	Basic	3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	Through Hardware and Software Audits helps to identify systems that are in need for maintenance. On completion of maintenance provides on going audit to ensure they remain up to date and alert in case they are not.
Maintenance	Derived	3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Through Data Scans INSIGHT can help to check if the equipment under maintenance contains CUI data. IT teams can use this information to ensure the equipment is properly sanitized before going for off-site maintenance.
Maintenance	Derived	3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	
Maintenance	Derived	3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external	

			network connections and terminate such connections when nonlocal maintenance is complete.	
Maintenance	Derived	3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	
Media Protection	Basic	3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	GuardWare INSIGHT helps organisations ensure proper handling of their digital assets and the media used to store, access and transfer them through the automation of the following processes: • Helps in taking an inventory of the digital assets by performing data discovery scans to locate where sensitive data is stored. • Automatically classifies sensitive data which includes the requirements of handling Defence Information. • Passes usage reports of sensitive assets to information owners and to TCO (Technology Control Officer) in case of ITAR information. • Ensures proper use of sensitive assets by monitoring their access, usage, transfer, and storage. • Monitors movement of data on all offline sources like USBs, phone sync and online encrypted channels like personal cloud, social media, chat, and emails. • Provides ability to control data transfer channels, which include offline media and online cloud storage sources. • Helps to enforce policies on mobile devices and work from home scenarios when users are not connected to the corporate network.
Media Protection	Basic	3.8.2	Limit access to CUI on system media to authorized users	
Media Protection	Basic	3.8.3	Sanitize or destroy system media containing CUI before disposal or release for reuse.	
Media Protection	Derived	3.8.4	Mark media with necessary CUI markings and distribution limitations.	
Media Protection	Derived	3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	
Media Protection	Derived	3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by	

			alternative physical safeguards.	
Media Protection	Derived	3.8.7	Control the use of removable media on system components.	
Media Protection	Derived	3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	
Media Protection	Derived	3.8.9	Protect the confidentiality of backup CUI at storage locations.	
Personnel Security	Basic	3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	
Personnel Security	Basic	3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers	• GuardWare INSIGHT is an integral component during staff turnover, to enforce confidentiality of information taken by staff members during their employment. • GuardWare INSIGHT monitors user behaviours and alerts in the event of risky actions by users, and when they go against company policies. • Helps to enforce access controls on sensitive data once the user moves to a different department or project. • GuardWare INSIGHT helps in the implementation of the Trusted Insider Programme, as per the requirements of DSPF and DISP. It implements the Trusted Insider controls as per the ACSC ISM. • The detected incidents are used by company's IT security teams to educate the users about where they have gone wrong, raise their awareness towards cyber security, and in the case of malicious activity take disciplinary actions.
Physical Protection	Basic	3.10.1	Limit physical access to organizational systems, equipment, and the respective operating	

			environments to authorized individuals.	
Physical Protection	Basic	3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	
Physical Protection	Derived	3.10.3	Escort visitors and monitor visitor activity.	
Physical Protection	Derived	3.10.4	Maintain audit logs of physical access.	
Physical Protection	Derived	3.10.5	Control and manage physical access devices.	
Physical Protection	Derived	3.10.6	Enforce safeguarding measures for CUI at alternate work sites.	

Risk Assessment	Basic	3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI	GuardWare INSIGHT helps to automate many facets of risk and security assessments. The risk report from GuardWare INSIGHT becomes an integral part of closing the security gaps in a company. • GuardWare INSIGHT helps with the identification, classification and proper handling of sensitive data. This includes compliance to contractual obligations, standards, defence and privacy regulations. • GuardWare INSIGHT offers specialised capabilities and reports that help to test the security and risk posture of a company on an on-going basis. It does this by allowing users to define various risks, security controls and their severity levels in a digital risk register. • Once defined, advanced analytics and machine learning are used to monitor the usage of CUI and the users' behaviour (over a period of time) against the defined risks. This includes monitoring the usage pattern against peer groups, and also how changes in user behaviour occur over time. The system learns from these changes and highlights instances which are out of the ordinary. • A risk score is calculated based on each user interaction, which helps to highlight the top risk-causing user in a company and the types of risky actions that result in a high-risk score. This can be fed back into user training, and into any security adjustments required within a company's environment. • An overall security and risk assessment report is produced, which details the current risk posture of an entire company. The report allows the management to drill down on any identified risk and decide the appropriate actions to take to mitigate it.
Risk Assessment	Derived	3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	
Risk Assessment	Derived	3.11.3	Remediate vulnerabilities in accordance with risk assessments.	

Security Assessment	Basic	3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	• GuardWare INSIGHT offers specialised capabilities and reports that help to test the security and risk posture of a company on an on-going basis. It does this by allowing admin to define various risks, security controls and their severity levels in a digital risk register. • Once defined, advanced analytics and machine learning are used to monitor the usage of CUI and the users' behaviour (over a period of time) against the defined risks. This includes monitoring the usage pattern against peer groups, and also how changes in user behaviour occur over time. The system learns from these changes and highlights instances which are out of the ordinary. • A risk score is calculated based on each user interaction, which helps to highlight the top risk-causing user in a company and the types of risky actions that result in a high-risk score. This can be fed back into user training, and into any security adjustments required within a company's environment. • An overall security and risk assessment report is produced, which details the current risk posture of an entire company. The report allows the management to drill down on any identified risk and decide the appropriate actions to take to mitigate it. • INSIGHT helps to decentralise information security to information owners who understand the sensitivity of the information. Using INSIGHT, department heads/project managers/programme managers get reports on the usage of their data by their staff members. This helps to reduce detection time in case of non-compliance and increases speed of remediation. IT Security focuses on facilitating this workflow and monitors data and processes that are applicable across the entire organisation.
Security Assessment	Basic	3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	
Security Assessment	Basic	3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	
Security Assessment	Basic	3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.[28]	
System and Communications Protection	Basic	3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal	• GuardWare INSIGHT monitors all forms of offline and online communication channels. These include: o Any corporate sources like emails, teams, data sharing apps and SharePoint. o Offline sources like USBs, Bluetooth, print and phone sync. o Any non-corporate encrypted channels like free emails, cloud, websites, chat including WhatsApp, WeChat and Telegram.

			boundaries of organizational systems.	
System and Communications Protection	Basic	3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	• GuardWare INSIGHT offers several means of ensure secure and safe handling sensitive CUI Data. This includes: o Classification and monitoring of sensitive data o Monitoring and controlling access of sensitive data o Monitoring and restricting flow/transfer of CUI data to only defined means and applications o Controlling flow / transfer of CUI on all offline and online means o Controlling connections means o Ensuring the devices are up to date o Providing procedural workflows for proper identification, reporting and resolution of security incidents. o Providing various risk and AI based reports to quickly identify possible vulnerabilities and ensure their proper resolution. o Provide a system that facilitates and be the bedrock for and overall organisational security framework.
System and Communications Protection	Derived	3.13.3	Separate user functionality from system management functionality.	
System and Communications Protection	Derived	3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	The systems monitors and prevents the transfer of sensitive CUI data via any online or offline means.
System and Communications Protection	Derived	3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	

System and Communications Protection	Derived	3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	
System and Communications Protection	Derived	3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	
System and Communications Protection	Derived	3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	
System and Communications Protection	Derived	3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	
System and Communications Protection	Derived	3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	
System and Communications Protection	Derived	3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	

System and Communications Protection	Derived	3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.[29].	
System and Communications Protection	Derived	3.13.13	Control and monitor the use of mobile code.	
System and Communications Protection	Derived	3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	
System and Communications Protection	Derived	3.13.15	Protect the authenticity of communications sessions.	
System and Communications Protection	Derived	3.13.16	Protect the confidentiality of CUI at rest.	Helps in taking an inventory of the digital assets by performing data discovery scans to locate where sensitive data is stored. Once detected organisations can take appropriate action to secure the data at rest.
System and Information Integrity	Basic	3.14.1	Identify, report, and correct system flaws in a timely manner.	• Operationalizes the monitoring required for CUI related data • INSIGHT helps to ensure the correct processes (for handling data and reviewing incidents) are being followed.
System and Information Integrity	Basic	3.14.2	Provide protection from malicious code at designated locations within organizational systems.	

System and Information Integrity	Basic	3.14.3	Monitor system security alerts and advisories and take action in response.	• The system provides logs of all incidents, as well as logs of administrators and their duties. • Reports on the number of active incidents. • The system provides workflow management for reported incidents. Incidents can be routed (based on their type) to relevant information owners, CSOs or TCO (Technology Control Officers) in case of ITAR. The system provides excel based reporting to information owners for ease of use. Information owners are provided with access accounts to the system and to the relevant incidents. They can review the incidents and decide if they require further action or should be closed, by selecting the appropriate option in the system.
System and Information Integrity	Derived	3.14.4	Update malicious code protection mechanisms when new releases are available.	
System and Information Integrity	Derived	3.14.5	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	Provides monitoring and alerting against the use of non-organisational applications. This includes APPs that don't require admin rights to run.
System and Information Integrity	Derived	3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Provides monitoring of all outbound traffic via any installed or online application and alerts if sensitive data (CUI) is transferred and is under risk.
System and Information Integrity	Derived	3.14.7	Identify unauthorized use of organizational systems.	Provide complete monitoring of devices and data from user and device perspective.