SOFTWARE HOUSE

From Tyco Security Products

FISMA-Ready

C•CURE 9000 System

SOFTWARE HOUSE
From Tyco Security Products

DISCLAIMER

This document is being provided for informational purposes only, and is not intended as, and shall not constitute, legal advice. Compliance with any law or regulation is solely the responsibility of the user, and Tyco strongly cautions users to seek the advice of qualified legal counsel on such matters. The inclusion of information herein shall not be considered a determination that any portion of any law or regulation is applicable to any specific user or that the implementation of any of the system configuration settings discussed herein will bring a user or their system into full compliance with any law or regulation. This document is current as of its date of issuance, and Tyco does not undertake any obligation to update or supplement the information contained herein due to any changes in law, regulation or otherwise.

THIS DOCUMENT IS BEING PROVIDED "AS IS", WITHOUT REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TYCO EXPRESSLY DISCLAIMS ANY AND ALL SUCH WARRANTIES (INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY), FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL TYCO BE LIABLE FOR ANY DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOSS OF FUTURE SALES, LOSS OF PROFITS OR GOODWILL, LOSS OF DATA OR LOSS OF USE. The foregoing disclaimers and limitations shall apply to the maximum extent permitted by applicable law.

SOFTWARE HOUSE
From Tyco Security Products

Synopsis

This document provides an overview of the Tyco Security Products' FISMA-Ready Program and describes how the C•CURE 9000 System may be configured to meet the requirements of the Federal Information Security Management Act (FISMA). When used in conjunction with the C•CURE 9000 installation and configuration guides, this information will assist in the installation of a FISMA-compliant system and provide the necessary information for a FISMA audit.

Contents

SOFTWARE HOUSE
From Tyco Security Products

The FISMA-Ready Program

Title III of the E-Government Act of 2002, known as the Federal Information Security Management Act (FISMA), requires federal agencies to implement information security programs. FISMA compliance is the responsibility of the Organization[1], but many of the requirements are dependent on the devices and software used.

Tyco Security Products' FISMA-Ready Program was initiated to develop systems capable of being configured to meet the requirements of FISMA. Its goal is to provide the information and documentation necessary for the system to be configured into a compliant state and provide documentation necessary to assist in a FISMA audit.

That information is given using the Risk Management Framework described in the National Institute of Standards and Technology (NIST) Special Publication 800-53. The Framework defines a process to determine a system's security category and select security controls. After the applicable controls have been identified, steps are taken to ensure compliance.

The C•CURE 9000 System was evaluated using the guidelines provided by NIST and in partnership with an independent security consultant to identify the applicable controls. A C•CURE 9000 System can be configured to comply with all applicable controls and to assist in meeting the controls needed for the installation.

[1] The term "Organization" as used in this document refers to the organization ultimately responsible for FISMA compliance.

SOFTWARE HOUSE
From Tyco Security Products

The Risk Management Framework

The Risk Management Framework is described in the NIST Special Publication 800-53 and provides a step-by-step process for maintaining and improving the security of a system and the environment in which it operates. It is intended to be used by the Organization to address the complete lifecycle of a system including design, development, implementation, operation, and disposal.

Tyco Security Products has taken responsibility for the first three steps of the framework for the C•CURE 9000 System. The results are described in this document.

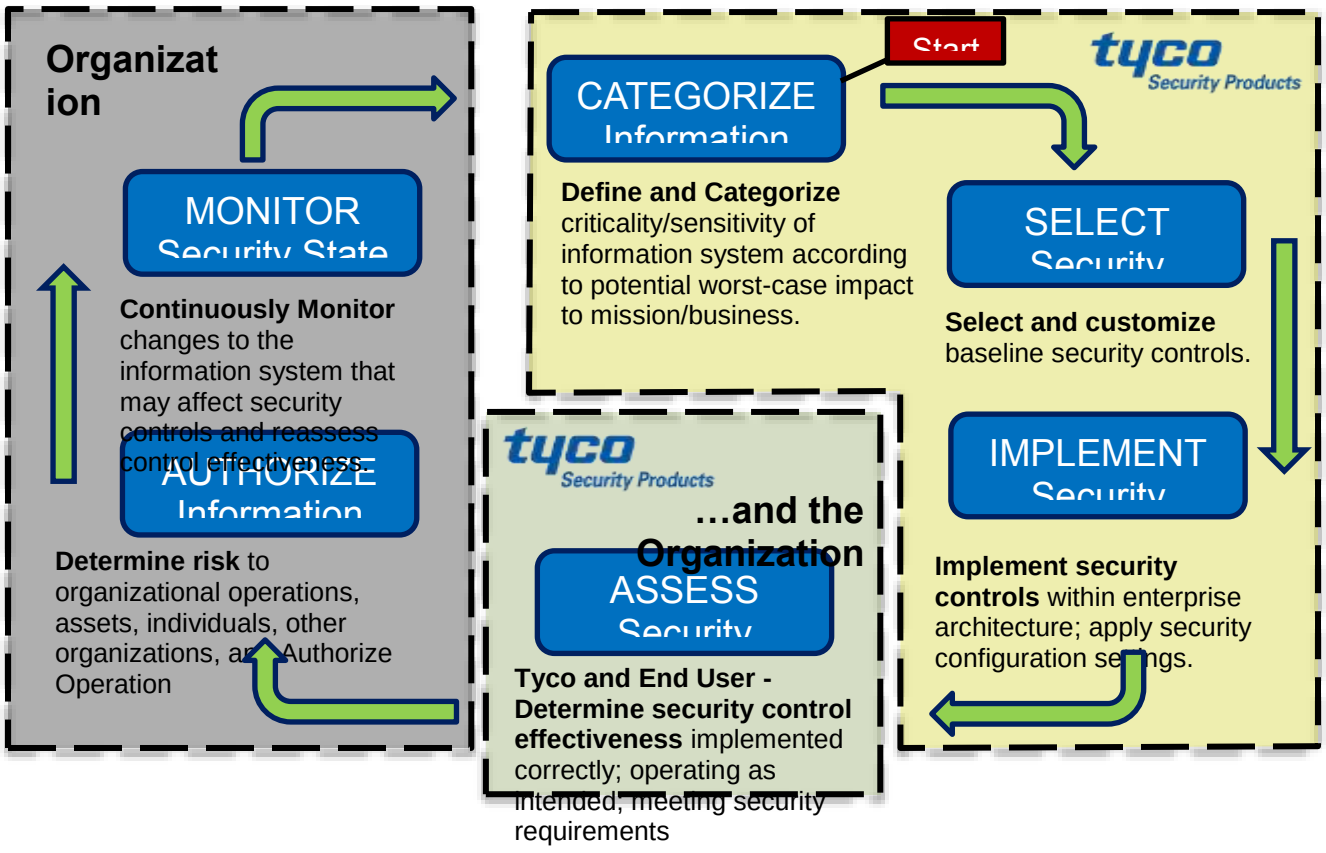

Fig.1 – The Risk Management Framework with shared responsibilities

To complete the cycle, feedback from the Organization on the effectiveness of the applied security controls is incorporated into another cycle of the framework process. Through this shared responsibility, implementation of the framework process yields continuous improvement of the overall security of the system.

Step 1 - Categorize:

The C•CURE 9000 System was independently assessed for the potential impact on an organization should a breach in security occur. This assessment was based on the Federal Information Processing Standard 199 (FIPS-199) and NIST Special Publication 800-60.

Impact levels are determined for each information type based on the three security objectives defined by FISMA:

> **Confidentiality** - "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]
>
> **Integrity** - "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]
>
> **Availability** - "Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]

Based on this assessment, the C•CURE 9000 System has been rated appropriate for an installation with overall security impact categorization of Moderate.

Information Type	Confidentiality	Integrity	Availability
Information Security	Low	Moderate	Low
System and Network Monitoring	Moderate	Moderate	Low
Security Management	Moderate	Moderate	Low

Criminal Investigation and Surveillance	Moderate	Moderate	Moderate
Property Protection	Low	Low	Low

The potential impact is LOW if:

− The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals.

The potential impact is MODERATE if:

− The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals.

The potential impact is HIGH if:

− The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals.

Step 2 – Select Controls:

The controls are categorized into eighteen families. Within each family are controls that pertain to the topic of that family. Controls may involve aspects of policy, oversight, supervision, manual processes, actions required by individuals, or automated mechanisms.

The list of applicable controls is derived from the determination of the security impact level in Step 1. For the C•CURE 9000 System, the controls were selected based on the Moderate impact level.

While overall compliance is the responsibility of the Organization, the C•CURE 9000 System has been designed to meet the requirements of certain controls that pertain to the devices and software within the system. The selection of these controls was done

through the guidelines of the NIST Special Publication 800-53 and from an independent assessment.

Technical Controls

Controls regarding the mechanisms of the hardware and software intended to protect the system from unauthorized access, disruption, and modification.

AC	Access Control*[2]
AU	Audit and Accountability*
IA	Identification and Authentication*
SC	System and Communications Protection*

Operational Controls

Controls employed by the Organization to support the management of the security controls. These controls are typically executed by people instead of systems, but often require the support of the system to be effective.

AT	Awareness and Training
CM	Configuration Management
CP	Contingency Planning*
IR	Incident Response
MA	Maintenance
MP	Media Protection*
PE	Physical and Environmental Protection
PS	Personnel Security
SI	System and Information Integrity*

Management Controls

Controls employed by the Organization to manage the security of the system, the Organization's assets, and operations. These controls are not executed by the system.

CA	Security Assessment and Authorization
PL	Planning
RA	Risk Assessment Management

[2] Asterisk (*) indicates a compliant response for the C•CURE 9000 system is available.

SA System and Services Acquisition
PM Program Management

Step 3 – Implement Controls

After the applicable controls were identified, the process of implementing the controls into the C•CURE 9000 System was started. Some controls are developed into the background function. For example, C•CURE 9000 Systems support encrypted remote sessions.

AC-17.2	The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.	**Compliant –** C•CURE 9000 supports SSL connections for remote sessions.

Other controls require C•CURE 9000 to be configured at installation. For example, C•CURE 9000 can be configured to separate duties, but it is the responsibility of the Organization to setup and configure these roles within the system. C•CURE 9000 user documentation describes how to implement this feature.

AC-2.7	The organization: a. Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and b. Tracks and monitors privileged role assignments.	**Compliant -** Responsibility for this control is shared by the organization and the system. In support of role-based access control, C•CURE 9000 is capable of creating user accounts with different privileges and permissions associated with role types. C•CURE 9000 logs account and role changes.

Every applicable control has been provided with a response to how a C•CURE 9000 System can be used to meet the requirements. For consistency, every control within the applicable families has been included, even if the control does not apply to the C•CURE 9000 System itself. For example, it is the responsibility of the Organization to provide training to employees.

AT-3.1	The organization provides employees with initial and [Assignment: organization-defined frequency][3] training in the employment and operation of environmental controls.	**Not Applicable -** This control is the responsibility of the organization.

Where a control is not applicable, but the C•CURE 9000 System can support the Organization in meeting the requirements, details are provided. For example, it is the responsibility of the Organization to analyze audit records, but C•CURE 9000 can support that effort by generating the necessary logs.

AU-6.3	The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	**Not Applicable -** This control is the responsibility of the organization. The logs generated by C•CURE 9000 can be used to support this control.

[3] Text contained within brackets in a control is the responsibility of the Organization to define. In this example, the Organization must define the frequency of training.

APPENDIX A – FISMA-Ready Controls

Control	Requirement	C•CURE 9000
	ACCESS CONTROL	
AC-1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.	**Not Applicable -** The organization is responsible for determining the access control policy and procedures. C•CURE 9000 functionality supports access control policies.
AC-2	The organization manages information system accounts, including: a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); b. Establishing conditions for group membership; c. Identifying authorized users of the information system and specifying access privileges; d. Requiring appropriate approvals for requests to establish accounts; e. Establishing, activating, modifying, disabling, and removing accounts; f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; g. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users; i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and j. Reviewing accounts [Assignment: organization-defined frequency].	**Compliant -** Responsibility for this control is shared by the organization and the system. System accounts are managed using the operating system for system level access. Accounts are grouped into role-based access permissions. Access to the information system requires authentication prior to granting access. Guest accounts are disabled.

Control	Requirement	C•CURE 9000
AC-2.1	The organization employs automated mechanisms to support the management of information system accounts.	**Compliant -** C•CURE 9000 provides a user interface that provides administrators with the ability to create and manage operator accounts. Each operator account can be configured individually with designated privileges, credentials and attributes. C•CURE 9000 operator accounts are also associated with Windows user accounts. C•CURE 9000 can be joined to an Active Directory domain which supports automated account management.
AC-2.2	The information system automatically terminates temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].	**Compliant -** To support this control, C•CURE 9000 relies on the functionality of Microsoft Active Directory and must be part of a Windows Active Directory Domain. C•CURE 9000 is capable of joining an Active Directory domain which supports automated account management. C•CURE 9000 can be joined to the organization's Active Directory domain. Support for this control is shared by C•CURE 9000 and the organization's IT infrastructure.
AC-2.3	The information system automatically disables inactive accounts after [Assignment: organization-defined time period].	**Compliant -** User accounts can be manually disabled. Neither C•CURE 9000 nor Active Directory support automatic disabling of user accounts based on inactivity. Administrators can schedule the time at which an account becomes disabled. An Administrator has the ability to configure an account as follows: - Account can be disabled by default by configuration. - A C•CURE operator account can be disabled independently from the Windows account. - An account expiration date can be established. - An operator user account has a password expiration policy which can be managed by the administrator.
AC-2.4	The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.	**Compliant -** C•CURE 9000 supports this control. C•CURE 9000 has audit logging turned on by default. C•CURE 9000 can be configured to logs the events covered by this control. Certain, but not all, events can trigger notifications to appropriate individuals.

Control	Requirement	C•CURE 9000
AC-2.7	The organization: a. Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and b. Tracks and monitors privileged role assignments.	**Compliant -** Responsibility for this control is shared by the organization and the system. In support of role-based access control, C•CURE 9000 is capable of creating user accounts with different privileges and permissions associated with role types. C•CURE 9000 logs account and role changes.
AC-3	The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.	**Compliant -** The organization is responsible for determining the access control policy and procedures. C•CURE 9000 functionality supports access control policies.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	**Compliant -** This control is satisfied based on penetration testing of the environment.
AC-5	The organization: a. Separates duties of individuals as necessary to prevent malevolent activity without collusion; b. Documents separation of duties; and c. Implements separation of duties through assigned information system access authorizations.	**Compliant -** Responsibility for this control is shared by the organization and the system. C•CURE 9000 supports the separation of duties through three specific account types - System Administrator, Personnel Administrator and Guard -- as well as the capability to set individual account privileges for each account.
AC-6	The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	**Compliant -** C•CURE 9000 supports this control with its ability to configure individual privileges to each operator account at very granular levels. When an operator account is created, individual privileges or privilege groups (i.e., predefined groups of privileges) can be assigned to the operator account. C•CURE 9000 is based on Object Relationship Model (ORM). Thus, all objects are “privileged” for Read, Edit and Action operations distinctly for each operator. Modifying the privileges can only be done by someone who has been granted "edit" access to the privileged object. Also, the operator would need the "Edit" privilege to Operator Objects in order to assign this privileges.
AC-6.1	The organization explicitly authorizes access to [Assignment: organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information].	**Not Applicable -** The organization is responsible for this control in accordance with organization's security function access policy.

Control	Requirement	C•CURE 9000
AC-6.2	The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined list of security functions or security-relevant information], use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.	**Compliant -** C•CURE 9000 supports the separation of duties as well as audit functionality. C•CURE 9000 supports this control with its ability to configure individual privileges for each operator account at very granular levels. C•CURE 9000 supports the configuration of multiple accounts with different privileges that can be allocated to a single user to support this control. The accounts can be created and configured according to the organizations needs during installation or subsequently.
AC-7	The information system: a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid login attempts by a user during a [Assignment: organization-defined time period]; and b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next login prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.	**Compliant -** In support of this control, C•CURE 9000 relies on the Windows operating system ability to manage account login and lockout functionality. C•CURE 9000 uses Windows authentication before connection is made to server. Thus, login attempts and recording mechanisms are subject to the organization's domain/IT policies and corresponding configuration. This control is also supported by C•CURE 9000's integration with Microsoft Active Directory. C•CURE 9000 is capable of joining an Active Directory domain which supports automated account login and lockout management.

Control	Requirement	C•CURE 9000
AC-8	The information system: a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.	**Compliant -** The Windows operating system supports the enabling and configuration of a banner screen with appropriate use notification message prior to access to the account login screen. Additionally, C•CURE 9000 has its own splash screen. Although its modification is not accessible to typical C•CURE operators, it could be changed by editing a file in a resource library. However, the C•CURE 9000 splash screen times out and disappears automatically without acknowledgement.
AC-10	The information system limits the number of concurrent sessions for each system account to [Assignment: organization-defined number].	**Compliant -** In support of this control, C•CURE 9000 relies on C•CURE 9000's integration with the Windows operating system, Windows authentication and Windows ability to manage sessions. Windows can be configured to restrict/limit using Windows group policy in accordance with the organization's configured domain/IT policies.

Control	Requirement	C•CURE 9000
AC-11	The information system: a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.	**Compliant -** In support of this control, C•CURE 9000 relies on the Windows operating system ability to manage enabling and disabling of a session lock. The session lock is maintained until the user reenters credentials to reestablish access. This control is also supported by C•CURE 9000's integration with Microsoft Active Directory. C•CURE 9000 is capable of joining an Active Directory domain which supports automated account login and lockout management. The System Administrator can configure the session lock inactivity time.
AC-11.1	The information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.	**Compliant -** C•CURE 9000 provides a session lock mechanism to disable viewing of the screen by displaying the login screen or another determined image other than the desktop.
AC-14	The organization: a. Identifies specific user actions that can be performed on the information system without identification or authentication; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.	**Compliant -** C•CURE 9000 prevents execution of user actions prior to identification and authentication.
AC-14.1	The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.	**Compliant -** C•CURE 9000 prevents execution of user actions prior to identification and authentication.
AC-17	The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections.	**Not Applicable -** The organization is responsible for remote access policies and authorizations. C•CURE 9000 supports remote access from system clients. Remote network access can be controlled using Windows host-supported mechanisms. Remote access to C•CURE 9000 can be accomplished through a VPN to the platform (i.e., hardware/OS) that hosts C•CURE 9000. The organization's network configuration and remote access mechanisms are responsible for permitting or restricting the establishment of a remote session with the platform that hosts C•CURE 9000.

Control	Requirement	C•CURE 9000
AC-17.1	The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.	**Compliant -** Responsibility for this control is shared by the organization and the system. C•CURE 9000 supports remote access from system clients. Remote network access can be controlled using Windows-supported mechanisms. Remote access to C•CURE 9000 can be accomplished through a VPN to the platform (i.e., hardware/OS) that hosts C•CURE 9000. The organization's network configuration and remote access mechanisms are responsible for permitting or restricting the establishment of a remote session with the platform that hosts C•CURE 9000.
AC-17.2	The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.	**Compliant -** C•CURE 9000 supports SSL connections for remote sessions.
AC-17.3	The information system routes all remote accesses through a limited number of managed access control points.	**Not Applicable -** This control is the responsibility of the organization. The organization is responsible for configuration of access control points. Remote network access to C•CURE 9000 can be controlled using Windows host-supported mechanisms.
AC-17.4	The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.	**Compliant -** Responsibility for this control is shared by the organization and the system. C•CURE 9000 supports the assignment of roles and privileges to user accounts.
AC-18	The organization: a. Establishes usage restrictions and implementation guidance for wireless access; b. Authorizes wireless access to the information system prior to allowing such connections.	**Not Applicable -** The C•CURE 9000 system assessment does not include wireless access.
AC-18.1	The information system protects wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.	**Not Applicable -** The C•CURE 9000 system assessment does not include wireless access.
AC-19	The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and b. Authorizes the connection of mobile devices to organizational information systems.	**Not Applicable -** The C•CURE 9000 system assessment does not include mobile device connections

Control	Requirement	C•CURE 9000
AC-19.5	The organization employs [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].	**Not Applicable -** The C•CURE 9000 system assessment does not include mobile device connections
AC-20	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from the external information systems; and b. Process, store, and/or transmit organization-controlled information using the external information systems.	**Not Applicable -** This control is the responsibility of the organization. Unauthorized external information systems should not be allowed to access C•CURE 9000.
AC-20.1	The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: a. Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or b. Has approved information system connection or processing agreements with the organizational entity hosting the external information system.	**Not Applicable -** This control is the responsibility of the organization. Unauthorized external information systems should not be allowed to access C•CURE 9000.
AC-20.2	The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.	**Not Applicable -** This control is the responsibility of the organization. Unauthorized external information systems should not be allowed to access C•CURE 9000.

Control	Requirement	C•CURE 9000
AC-22	The organization: a. Designates individuals authorized to post information onto an organizational information system that is publicly accessible; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system; d. Reviews the content on the publicly accessible organizational information system for nonpublic information [Assignment: organization-defined frequency]; and e. Removes nonpublic information from the publicly accessible organizational information system, if discovered.	**Compliant -** The responsibility for this control is shared by the organization and the technical controls provided by C•CURE 9000. Data from C•CURE 9000 is not publicly accessible. It is accessible only by authorized individuals who are assigned credentials and permissions in accordance with their role. The organization is responsible for using the technical controls supported by C•CURE 9000 and for enforcing the physical access restrictions to the system. Protection of the information maintained by C•CURE 9000 is critical to protecting the physical environment of the organization.
	AWARENESS AND TRAINING	
AT-1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	**Not Applicable -** This control is the responsibility of the organization.
AT-2	The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and [Assignment: organization-defined frequency] thereafter.	**Not Applicable -** This control is the responsibility of the organization.
AT-3	The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [Assignment: organization-defined frequency] thereafter.	**Not Applicable -** This control is the responsibility of the organization.
AT-3.1	The organization provides employees with initial and [Assignment: organization-defined frequency] training in the employment and operation of environmental controls.	**Not Applicable -** This control is the responsibility of the organization.

Control	Requirement	C•CURE 9000
AT-4	The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for [Assignment: organization-defined time period].	**Not Applicable -** This control is the responsibility of the organization.
	AUDIT AND ACCOUNTABILITY	
AU-1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	**Not Applicable -** This control is the responsibility of the organization.

Control	Requirement	C•CURE 9000
AU-2	The organization: a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [Assignment: organization-defined list of auditable events]; b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event].	**Compliant -** The responsibility for this control is shared by the organization and C•CURE 9000. In support of item (a) of this control, C•CURE 9000 logs -- or can be configured to log -- every configuration change and identifies which operator performed the function. C•CURE 9000 also logs all events supported by the system. The organization has primary responsibility for items (a), (b), (c) and (d) of this control. All object configuration changes are audited by C•CURE 9000. The following runtime activity types are written to the Journal database: User Login/Logout Card Admitted Card Rejected Log Message State Change Manual Action System Activity System Error Device Activity Device Error/Recovery NetVideo Activity Keypad Command Intrusion Zone Act. Intrusion Zone Error Area Activity
AU-2.3	The organization reviews and updates the list of auditable events [Assignment: organization-defined frequency].	**Not Applicable -** This control is the responsibility of the organization.
AU-2.4	The organization includes execution of privileged functions in the list of events to be audited by the information system.	**Compliant -** The responsibility for this control is shared by the organization and C•CURE 9000. C•CURE 9000 supports the assignment of privileged functions to user accounts and the auditing of user actions.

Control	Requirement	C•CURE 9000
AU-3	The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.	**Compliant -** The C•CURE 9000 Audit, Journaling and Event functions meet this control. CURE 9000 has built in audit log database within SQL Server. The audit log database is set up with SQL Server. All configuration based modifications including field level modifications are logged to the audit trail. Field level auditing is configurable by the user. All other modifications are automatically recorded. Audit database size, storage length of time, and number of messages is configurable by the user. Database backup location is also configurable. All runtime activity including Operator actions are recorded in the Journal database. Journal Database Size, storage length of time, and number of messages is configurable by the user. Database backup location is also configurable. Once defined log size is reached, a separate "log volume" is created. Actual database size limitation is part of Microsoft's SQL Server Solution.
AU-3.1	The information system generates audit records containing the following additional information: [Assignment: organization-defined additional, more detailed information].	**Compliant -** See control AU-2.
AU-4	The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	**Compliant -** The Log Volume Management settings are covered in the C•CURE 9000 Maintenance Guide. There are several settings available to the organization for managing the audit record storage capacity.

Control	Requirement	C•CURE 9000
AU-5	The information system: a. Alerts designated organizational officials in the event of an audit processing failure; and b. Takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].	**Compliant -** C•CURE 9000 supports this control through configuration of it Event and Journaling functions, the Windows operating system and SQL server. C•CURE 9000 Utilizes SQL Server Database. Thus, the limitations are typically setup by IT or DB Admin. C•CURE 9000 does have a facility to backup database by Event, Schedule, or Manual operation. Also, C•CURE 9000 can trigger a backup if a configurable "Max Size" limit has been reached. Journaling entries are written to a SQL server. C•CURE 9000 can detect if the SQL service fails. C•CURE 9000 can be configured to only append records. Audit and Journal logs cannot be overwritten or modified by the system. It is the organization's responsibility to use the Windows OS and possibly other IT tools to monitor the status of C•CURE 9000 server components to trigger alerts to organization officials in case of failure. It is assumed that the organization's network infrastructure and email system can support this capability.
AU-6	The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.	**Not Applicable -** This control is the responsibility of the organization.

Control	Requirement	C•CURE 9000
AU-6.1	The information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.	**Compliant -** The responsibility for this control is shared by the organization and VE NVR. C•CURE 9000 supports this control by providing a set of pre-defined reports, queries and views of audited and journaled system events. Users can also create customized event reports based on selected criteria. Queries can be built around database modifications. For example, users can search what changes particular individuals made. Or the user can search on "types" of changes to investigate suspicious activity. Similar capabilities are available with the Journal Database.
AU-6.3	The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	**Not Applicable -** This control is the responsibility of the organization. The logs generated by C•CURE 9000 can be used to support this control.
AU-7	The information system provides an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and b. Does not alter the original content or time ordering of audit records.	**Compliant -** C•CURE 9000's Audit Query and Journal Query functions support this control.
AU-7.1	The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.	**Compliant -** C•CURE 9000's Audit Query and Journal Query functions support this control.
AU-8	The information system uses internal system clocks to generate time stamps for audit records.	**Compliant -** C•CURE 9000 generates a timestamp for each audit and journal entry record. The Windows system clock is used as the timestamp. C•CURE 9000 provides multiple options for the configuring the system clock source time by which all system components can be synchronized.
AU-8.1	The information system synchronizes internal information system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source].	**Compliant -** C•CURE 9000 provides multiple options for the configuring the system clock source time by which all system components can be synchronized. This allows for the C•CURE environment to communicate and remain synchronized. C•CURE 9000 does not necessarily require connection to an NTP server.

Control	Requirement	C•CURE 9000
AU-9	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	**Compliant -** The C•CURE 9000 event and journal databases are write-only databases. Periodic cleanups can be performed only by specifically privileged C•CURE 9000 Administrator operators.
AU-11	The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	**Not Applicable -** This control is the responsibility of the organization In support of this control, C•CURE 9000 provides the configuration of the following relevant parameters: - Audit Volume Size - Maximum Message Size in Audit Log - Number Of Days To Store in Audit Log Audit and Journal Database Size, storage length of time, and number of messages is configurable by the user. The database backup location is also configurable and can separated for 90 days of time. Length of time for online data is dependent on the volume of data occurring on site and acceptable query performance within SQL server. Recovery of backed up database can be performed through SQL database restore operation on a separate server. Policy and configuration is typically maintained by onsite IT department or DB Admin.
AU-12	The information system: a. Provides audit record generation capability for the list of auditable events defined in AU-2 at [Assignment: organization-defined information system components]; b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.	**Compliant -** In support of this control, C•CURE 9000 logs -- or can be configured to log -- every configuration change. C•CURE 9000 also logs all events supported by the system through its Journal Messaging system. Journal messages include the source identity of the configuration changes and events. The Journal Trigger function provides the capability to create reports based configured Journal Triggers associated with logged messages. C•CURE 9000's Dynamic Viewer function provides the ability to query the audit log based on user-defined criteria. C•CURE 9000 provide numerous other methods for customized reporting and viewing journal and audit log entries that are linked to system events.

Control	Requirement	C•CURE 9000
	SECURITY ASSESSMENT AND AUTHORIZATION	
CA-1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.	**Not Applicable -** This control is the responsibility of the organization.
CA-2	The organization: a. Develops a security assessment plan that describes the scope of the assessment including: -Security controls and control enhancements under assessment; -Assessment procedures to be used to determine security control effectiveness; and -Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.	**Compliant -** This organization and C•CURE 9000 share responsibility for this control. Tyco Security Products is prepared to support this control with: - Responses to security controls that for which Tyco/SoftwareHouse as a component supplier has responsibility. - Product documentation that supports creation of a system security plan. This documentation includes a C•CURE 9000 Cyber Security Hardening Guide.
CA-2.1	The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.	**Not Applicable -** This control is the responsibility of the organization. **Note:** Tyco Security Products Can support this control with documentation that supports the configuration of the C•CURE 9000 security controls.

Control	Requirement	C•CURE 9000
CA-3	The organization: a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements; b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.	**Not Applicable -** This control is the responsibility of the organization.
CA-5	The organization: a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	**Not Applicable -** This control is the responsibility of the organization.
CA-6	The organization: a. Assigns a senior-level executive or manager to the role of authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization [Assignment: organization-defined frequency].	**Not Applicable -** This control is the responsibility of the organization.
CA-7	The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: a. A configuration management process for the information system and its constituent components; b. A determination of the security impact of changes to the information system and environment of operation; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and d. Reporting the security state of the information system to appropriate organizational officials [Assignment: organization-defined frequency].	**Not Applicable -** This control is the responsibility of the organization.

Control	Requirement	C•CURE 9000
CA-7.2	The organization plans, schedules, and conducts assessments [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection: in-depth monitoring; malicious user testing; penetration testing; red team exercises; [Assignment: organization-defined other forms of security assessment]] to ensure compliance with all vulnerability mitigation procedures.	**Not Applicable -** This control is the responsibility of the organization.
	CONFIGURATION MANAGEMENT	
CM-1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	**Not Applicable -** This control is the responsibility of the organization.
CM-2	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	**Not Applicable -** This control is the responsibility of the organization. C•CURE 9000's baseline default configuration is documented within and throughout the system configuration documentation.
CM-2.1	The organization reviews and updates the baseline configuration of the information system: a. [Assignment: organization-defined frequency]; b. When required due to [Assignment organization-defined circumstances]; and c. As an integral part of information system component installations and upgrades.	**Not Applicable -** This control is the responsibility of the organization.
CM-2.2	The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, C•CURE 9000 provides functionality to back up the system.
CM-2.3	The organization retains older versions of baseline configurations as deemed necessary to support rollback.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, C•CURE 9000 provides functionality to backup and restore the system to a previous configuration baseline.

Control	Requirement	C•CURE 9000
CM-2.4	The organization: a. Develops and maintains [Assignment: organization-defined list of software programs not authorized to execute on the information system]; and b. Employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.	**Not Applicable -** The control is the responsibility of the organization. In support of this control, the C•CURE 9000 Installation and Upgrade Guide and Release notes provide information on limitations and compatibility with other software programs.
CM-3	The organization: a. Determines the types of changes to the information system that are configuration controlled; b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses; c. Documents approved configuration-controlled changes to the system; d. Retains and reviews records of configuration-controlled changes to the system; e. Audits activities associated with configuration-controlled changes to the system; and f. Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board] that convenes [Selection: (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].	**Not Applicable -** The control is the responsibility of the organization. C•CURE 9000 supports parts of this control through its system documentation and its Audit and Journal logging functions.
CM-3.2	The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.	**Not Applicable -** The control is the responsibility of the organization.
CM-3.4	The organization requires an information security representative to be a member of the [Assignment: organization-defined configuration change control element (e.g., committee, board)].	**Not Applicable -** The control is the responsibility of the organization.
CM-4	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	**Not Applicable -** The control is the responsibility of the organization. C•CURE 9000 supports this control through its system documentation.

Control	Requirement	C•CURE 9000
CM-5	The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, Tyco provides the C•CURE 9000 Cyber Security Hardening Guide which includes the hardening configuration options supported by C•CURE 9000.
CM-6	The organization: a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, Tyco provides the C•CURE 9000 Cyber Security Hardening Guide which includes hardening configurations functions supported by C•CURE 9000.
CM-7	The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services].	**Compliant -** Responsibility for this control is shared by the organization and the system. In support of this control, C•CURE 9000 is designed to enable and employ only those ports, protocols and services required to support the application.
CM-7.1	The organization reviews the information system [Assignment: organization-defined frequency] to identify and eliminate unnecessary functions, ports, protocols, and/or services.	**Compliant -** Responsibility for this control is shared by the organization and the system. In support of this control, C•CURE 9000 is designed to enable and employ only those ports, protocols and services required to support the application.
CM-7.2	The organization employs automated mechanisms to prevent program execution in accordance with [Selection (one or more): list of authorized software programs; list of unauthorized software programs; rules authorizing the terms and conditions of software program usage].	**Not Applicable -** This control is the responsibility of the organization. In support of this control, the C•CURE 9000 Installation and Upgrade Guide and Release notes provide information on limitations and compatibility with other software programs.
CM-7.3	The organization ensures compliance with [Assignment: organization-defined registration requirements for ports, protocols, and services].	**Not Applicable -** This control is the responsibility of the organization.

Control	Requirement	C•CURE 9000
CM-8	The organization develops, documents, and maintains an inventory of information system components that: a. Accurately reflects the current information system; b. Is consistent with the authorization boundary of the information system; c. Is at the level of granularity deemed necessary for tracking and reporting; d. Includes [Assignment: organization-defined information deemed necessary to achieve effective property accountability]; and e. Is available for review and audit by designated organizational officials.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, the organization may receive from the supplier the inventory of information system components that comprise the C•CURE 9000 system.
CM-8.1	The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, the organization may receive from the supplier the inventory of information system components that comprise the C•CURE 9000 system.
CM-8.3	The organization: a. Employs automated mechanisms [Assignment: organization-defined frequency] to detect the addition of unauthorized components/devices into the information system; and b. Disables network access by such components/devices or notifies designated organizational officials.	**Compliant -** Responsibility for this control is shared by the organization and the system. In support of this control, the C•CURE 9000 license manager tracks authorized products.
CM-8.5	The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, the organization may receive from the supplier the inventory of information system components that comprise the C•CURE 9000 system. Continuous maintenance of the system component inventory is the responsibility of the organization.

Control	Requirement	C•CURE 9000
CM-9	The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.	**Not Applicable -** This control is the responsibility of the organization.
	CONTINGENCY PLANNING	
CP-1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	**Not Applicable -** This control is the responsibility of the organization.

Control	Requirement	C•CURE 9000
CP-2	The organization: a. Develops a contingency plan for the information system that: - Identifies essential missions and business functions and associated contingency requirements; - Provides recovery objectives, restoration priorities, and metrics; -Addresses contingency roles, responsibilities, assigned individuals with contact information; -Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; -Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the contingency plan to [Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency]; e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and f. Communicates contingency plan changes to [Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements].	**Not Applicable -** This control is the responsibility of the organization.
CP-2.1	The organization coordinates contingency plan development with organizational elements responsible for related plans.	**Not Applicable -** This control is the responsibility of the organization.
CP-2.3	The organization plans for the resumption of essential missions and business functions within [Assignment: organization-defined time period] of contingency plan activation.	**Not Applicable -** This control is the responsibility of the organization.
CP-2.8	The organization identifies critical information system assets supporting essential missions and business functions.	**Not Applicable -** This control is the responsibility of the organization.

Control	Requirement	C•CURE 9000
CP-3	The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [Assignment: organization-defined frequency].	**Not Applicable -** This control is the responsibility of the organization.
CP-4	The organization: a. Tests and/or exercises the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests and/or exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan; and b. Reviews the contingency plan test/exercise results and initiates corrective actions.	**Not Applicable -** This control is the responsibility of the organization.
CP-4.1	The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.	**Not Applicable -** This control is the responsibility of the organization.
CP-6	The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information.	**Not Applicable -** This control is the responsibility of the organization.
CP-6.1	The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards.	**Not Applicable -** This control is the responsibility of the organization.
CP-6.3	The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	**Not Applicable -** This control is the responsibility of the organization.
CP-7	The organization: a. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [Assignment: organization-defined time period consistent with recovery time objectives] when the primary processing capabilities are unavailable; and b. Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption.	**Not Applicable -** This control is the responsibility of the organization.
CP-7.1	The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.	**Not Applicable -** This control is the responsibility of the organization.

Control	Requirement	C•CURE 9000
CP-7.2	The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	**Not Applicable -** This control is the responsibility of the organization.
CP-7.3	The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.	**Not Applicable -** This control is the responsibility of the organization.
CP-8	The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable.	**Not Applicable -** This control is the responsibility of the organization.
CP-8.1	The organization: a. Develops primary and alternate telecommunications service agreements that contain priority of-service provisions in accordance with the organization's availability requirements; and b. Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.	**Not Applicable -** This control is the responsibility of the organization.
CP-8.2	The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.	**Not Applicable -** This control is the responsibility of the organization.
CP-9	The organization: a. Conducts backups of user-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; c. Conducts backups of information system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and d. Protects the confidentiality and integrity of backup information at the storage location.	**Compliant -** Responsibility for this control is shared by the organization and the system. In support of this control, C•CURE 9000 provides functionality to backup and restore user-level and system-level information.

Control	Requirement	C•CURE 9000
CP-9.1	The organization tests backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.	**Not Applicable -** This control is the responsibility of the organization.
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, C•CURE 9000 provides backup and restore functionality and documented procedures with the system manuals.
CP-10.2	The information system implements transaction recovery for systems that are transaction-based.	**Compliant -** C•CURE 9000's backup, restore, Audit and Journal functions provide the information to recover transactions.
	IDENTIFICATION AND AUTHENTICATION	
IA-1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	**Not Applicable -** This control is the responsibility of the organization.
IA-2	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	**Compliant -** C•CURE 9000 meets the technical requirements for this implementation. C•CURE 9000 complies with Homeland Security Presidential Directive 12 (HSPD-12).
1A-2.1	The information system uses multifactor authentication for network access to privileged accounts.	**Compliant -** C•CURE 9000 meets the technical requirements for this implementation. C•CURE 9000 complies with Homeland Security Presidential Directive 12 (HSPD-12).
IA-2.2	The information system uses multifactor authentication for network access to non-privileged accounts.	**Compliant -** C•CURE 9000 meets the technical requirements for this implementation. C•CURE 9000 complies with Homeland Security Presidential Directive 12 (HSPD-12).
IA-2.3	The information system uses multifactor authentication for local access to privileged accounts.	**Compliant -** C•CURE 9000 meets the technical requirements for this implementation. C•CURE 9000 complies with Homeland Security Presidential Directive 12 (HSPD-12).

Control	Requirement	C•CURE 9000
IA-2.8	The information system uses [Assignment: organization-defined replay-resistant authentication mechanisms] for network access to privileged accounts.	**Compliant -** C•CURE 9000 meets the technical requirements for this implementation. C•CURE 9000 complies with Homeland Security Presidential Directive 12 (HSPD-12).
IA-2.9	The information system uses [Assignment: organization-defined replay-resistant authentication mechanisms] for network access to non-privileged accounts.	**Compliant -** C•CURE 9000 meets the technical requirements for this implementation. C•CURE 9000 complies with Homeland Security Presidential Directive 12 (HSPD-12).
IA-3	The information system uniquely identifies and authenticates [Assignment: organization-defined list of specific and/or types of devices] before establishing a connection.	**Compliant -** C•CURE 9000 meets the technical requirements for this implementation.
IA-4	The organization manages information system identifiers for users and devices by: a. Receiving authorization from a designated organizational official to assign a user or device identifier; b. Selecting an identifier that uniquely identifies an individual or device; c. Assigning the user identifier to the intended party or the device identifier to the intended device; d. Preventing reuse of user or device identifiers for [Assignment: organization-defined time period]; and e. Disabling the user identifier after [Assignment: organization-defined time period of inactivity].	**Not Applicable -** This control is the responsibility of the organization.

Control	Requirement	C•CURE 9000
IA-5	The organization manages information system authenticators for users and devices by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators upon information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); g. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type]; h. Protecting authenticator content from unauthorized disclosure and modification; and i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.	**Compliant -** Responsibility for this control is shared by the organization and the system. In support of this control, C•CURE 9000 provides mechanisms to support this control.
IA-5.1	The information system, for password-based authentication: a. Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type]; b. Enforces at least a [Assignment: organization-defined number of changed characters] when new passwords are created; c. Encrypts passwords in storage and in transmission; d. Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; and e. Prohibits password reuse for [Assignment: organization-defined number] generations.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, C•CURE 9000 provides mechanisms to support this control.

Control	Requirement	C•CURE 9000
IA-5.2	The information system, for PKI-based authentication: a. Validates certificates by constructing a certification path with status information to an accepted trust anchor; b. Enforces authorized access to the corresponding private key; and c. Maps the authenticated identity to the user account.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, C•CURE 9000 host platforms may provide mechanisms to support this control.
IA-5.3	The organization requires that the registration process to receive [Assignment: organization-defined types of and/or specific authenticators] be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).	**Not Applicable -** This control is the responsibility of the organization.
IA-6	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	**Compliant -** C•CURE 9000 obscures user passwords when they are being input for authentication.
IA-7	The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	**Compliant -** C•CURE 9000 provides FIPS 140-2 Level 2 protection and authentication.
IA-8	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	**Compliant -** Responsibility for this control is shared by the organization and the system. C•CURE 9000 is capable of providing unique identification for non-organizational users. It is the responsibility of the organization to configure the systems to support this requirement.
	INCIDENT RESPONSE	
IR-1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.	**Not Applicable -** This control is the responsibility of the organization.

Control	Requirement	C•CURE 9000
IR-2	The organization: a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and b. Provides refresher training [Assignment: organization-defined frequency].	**Not Applicable -** This control is the responsibility of the organization.
IR-3	The organization tests and/or exercises the incident response capability for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests and/or exercises] to determine the incident response effectiveness and documents the results.	**Not Applicable -** This control is the responsibility of the organization.
IR-3.2	The organization coordinates incident response testing with organizational elements responsible for related plans.	**Not Applicable -** This control is the responsibility of the organization.
IR-4	The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.	**Not Applicable -** This control is the responsibility of the organization.
IR-4.1	The organization employs automated mechanisms to support the incident handling process.	**Not Applicable -** This control is the responsibility of the organization.
IR-5	The organization tracks and documents information system security incidents.	**Not Applicable -** This control is the responsibility of the organization.
IR-6	The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time-period]; and b. Reports security incident information to designated authorities.	**Not Applicable -** This control is the responsibility of the organization.
IR-6.1	The organization employs automated mechanisms to assist in the reporting of security incidents.	**Not Applicable -** This control is the responsibility of the organization.

Control	Requirement	C•CURE 9000
IR-7	The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	**Not Applicable -** This control is the responsibility of the organization.
IR-7.1	The organization employs automated mechanisms to increase the availability of incident response-related information and support.	**Not Applicable -** This control is the responsibility of the organization.
IR-8	The organization: a. Develops an incident response plan that: - Provides the organization with a roadmap for implementing its incident response capability; - Describes the structure and organization of the incident response capability; - Provides a high-level approach for how the incident response capability fits into the overall organization; - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; - Defines reportable incidents; - Provides metrics for measuring the incident response capability within the organization. - Defines the resources and management support needed to effectively maintain and mature an incident response capability; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the incident response plan to [Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [Assignment: organization-defined frequency]; d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and e. Communicates incident response plan changes to [Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements].	**Not Applicable -** This control is the responsibility of the organization.
	MAINTENANCE	

Control	Requirement	C•CURE 9000
MA-1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	**Not Applicable -** This control is the responsibility of the organization.
MA-2	The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.	**Not Applicable -** This control is the responsibility of the organization. C•CURE 9000 provides mechanisms that support some of these activities.
MA-2.1	The organization maintains maintenance records for the information system that include: a. Date and time of maintenance; b. Name of the individual performing the maintenance; c. Name of escort, if necessary; d. A description of the maintenance performed; and e. A list of equipment removed or replaced (including identification numbers, if applicable).	**Not Applicable -** This control is the responsibility of the organization.

Control	Requirement	C•CURE 9000
MA-3	The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, C•CURE 9000 permits only privileged user accounts to install diagnostic or external software on C•CURE 9000. Most diagnostics are built within the host operating system. C•CURE 9000 software updates and patches follow Tyco's release development process and are qualified before being released from manufacturing.
MA-3.1	The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.	**Not Applicable -** This control is the responsibility of the organization.
MA-3.2	The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, Tyco can provide any applicable software to the customer organization for checking prior to usage.
MA-4	The organization: a. Authorizes, monitors, and controls non-local maintenance and diagnostic activities; b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions; d. Maintains records for non-local maintenance and diagnostic activities; and e. Terminates all sessions and network connections when non-local maintenance is completed.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, the C•CURE 9000 manuals provide information on availability and use of any non-local maintenance and diagnostic connections. Remote access to C•CURE 9000 can be accomplished through a VPN to the platform (i.e., hardware/OS) that hosts C•CURE 9000. The organization's network configuration and remote access mechanisms are responsible for permitting or restricting the establishment of a remote session with the C•CURE 9000's host platform.

Control	Requirement	C•CURE 9000
MA-4.2	The organization documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, the C•CURE 9000 manuals provide information on availability and use of any non-local maintenance and diagnostic connections. Remote access to C•CURE 9000 can be accomplished through a VPN to the platform (i.e., hardware/OS) that hosts C•CURE 9000. The organization's network configuration and remote access mechanisms are responsible for permitting or restricting the establishment of a remote session with the platform that hosts C•CURE 9000.
MA-5	The organization: a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.	**Not Applicable -** This control is the responsibility of the organization. Tyco can provide a list of authorized C•CURE 9000 integrators to the organization.
MA-6	The organization obtains maintenance support and/or spare parts for [Assignment: organization-defined list of security-critical information system components and/or key information technology components] within [Assignment: organization-defined time period] of failure.	**Not Applicable -** This control is the responsibility of the organization. Tyco and/or its authorized integrators can provide maintenance support and spare parts.
	MEDIA PROTECTION	
MP-1	**Not Applicable -** This control is the responsibility of the organization.	**Not Applicable -** This control is the responsibility of the organization.
MP-2	The organization restricts access to [Assignment: organization-defined types of digital and non-digital media] to [Assignment: organization-defined list of authorized individuals] using [Assignment: organization-defined security measures].	**Not Applicable -** This control is the responsibility of the organization.

Control	Requirement	C•CURE 9000
MP-3	The organization: a. Marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts [Assignment: organization-defined list of removable media types] from marking as long as the exempted items remain within [Assignment: organization-defined controlled areas].	**Not Applicable -** This control is the responsibility of the organization.
MP-4	The organization: a. Physically controls and securely stores [Assignment: organization-defined types of digital and non-digital media] within [Assignment: organization-defined controlled areas] using [Assignment: organization-defined security measures]; b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	**Not Applicable -** This control is the responsibility of the organization.
MP-5	The organization: a. Protects and controls [Assignment: organization-defined types of digital and non-digital media] during transport outside of controlled areas using [Assignment: organization-defined security measures]; b. Maintains accountability for information system media during transport outside of controlled areas; and c. Restricts the activities associated with transport of such media to authorized personnel.	**Not Applicable -** This control is the responsibility of the organization.
MP-6	The organization: a. Sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and b. Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.	**Not Applicable -** This control is the responsibility of the organization.
MP-6.1	The organization tracks, documents, and verifies media sanitization and disposal actions.	**Not Applicable -** This control is the responsibility of the organization.
MP-6.2	The organization tests sanitization equipment and procedures to verify correct performance [Assignment: organization-defined frequency].	**Not Applicable -** This control is the responsibility of the organization.

Control	Requirement	C•CURE 9000
MP-6.3	The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: [Assignment: organization-defined list of circumstances requiring sanitization of portable, removable storage devices].	**Not Applicable -** This control is the responsibility of the organization.
	PHYSICAL AND ENVIRONMENTAL PROTECTION	
PE-1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	**Not Applicable -** This control is the responsibility of the organization.
PE-2	The organization: a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); b. Issues authorization credentials; c. Reviews and approves the access list and authorization credentials [Assignment: organization-defined frequency], removing from the access list personnel no longer requiring access.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, C•CURE 9000 user accounts can be enabled and disabled and configured with access privileges and permissions.

Control	Requirement	C•CURE 9000
PE-3	The organization: a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible); b. Verifies individual access authorizations before granting access to the facility; c. Controls entry to the facility containing the information system using physical access devices and/or guards; d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk; e. Secures keys, combinations, and other physical access devices; f. Inventories physical access devices [Assignment: organization-defined frequency]; and g. Changes combinations and keys [Assignment: organization-defined frequency] and when keys are lost, combinations are compromised, or individuals are transferred or terminated.	**Not Applicable -** This control is the responsibility of the organization.
PE-4	The organization controls physical access to information system distribution and transmission lines within organizational facilities.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, the organizations may use the C•CURE 9000 physical access control system as a mechanism for implementing this control.
PE-5	The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, the organizations may use the C•CURE 9000 physical access control system as a mechanism for implementing this control.
PE-6	The organization: a. Monitors physical access to the information system to detect and respond to physical security incidents; b. Reviews physical access logs [Assignment: organization-defined frequency]; and c. Coordinates results of reviews and investigations with the organization's incident response capability.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, the organizations may use the C•CURE 9000 physical access control system as a mechanism for implementing this control.

Control	Requirement	C•CURE 9000
PE-6.1	The organization monitors real-time physical intrusion alarms and surveillance equipment.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, the organizations may use the C•CURE 9000 physical access control system as a mechanism for implementing this control.
PE-7	The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, the organizations may use the C•CURE 9000 physical access control system as a mechanism for implementing this control.
PE-8	The organization: a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and b. Reviews visitor access records [Assignment: organization-defined frequency].	**Not Applicable -** This control is the responsibility of the organization. In support of this control, the organizations may use the C•CURE 9000 physical access control system as a mechanism for implementing this control.
PE-9	The organization protects power equipment and power cabling for the information system from damage and destruction.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, the organizations may use the C•CURE 9000 physical access control system as a mechanism for implementing this control.
PE-9.2	The organization employs automatic voltage controls for [Assignment: organization-defined list of critical information system components].	**Not Applicable -** This control is the responsibility of the organization.
PE-10	The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in [Assignment: organization-defined location by information system or system component] to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation.	**Not Applicable -** This control is the responsibility of the organization.
PE-11	The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.	**Not Applicable -** This control is the responsibility of the organization.

Control	Requirement	C•CURE 9000
PE-11.2	The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.	**Not Applicable -** This control is the responsibility of the organization.
PE-12	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	**Not Applicable -** This control is the responsibility of the organization.
PE-13	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	**Not Applicable -** This control is the responsibility of the organization.
PE-13.3	The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.	**Not Applicable -** This control is the responsibility of the organization.
PE-14	The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at [Assignment: organization-defined acceptable levels]; and b. Monitors temperature and humidity levels [Assignment: organization-defined frequency].	**Not Applicable -** This control is the responsibility of the organization.
PE-15	The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.	**Not Applicable -** This control is the responsibility of the organization.
PE-16	The organization authorizes, monitors, and controls [Assignment: organization-defined types of information system components] entering and exiting the facility and maintains records of those items.	**Not Applicable -** This control is the responsibility of the organization.
PE-17	The organization: a. Employs [Assignment: organization-defined management, operational, and technical information system security controls] at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.	**Not Applicable -** This control is the responsibility of the organization.

Control	Requirement	C•CURE 9000
	PLANNING	
PL-1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	**Not Applicable -** This control is the responsibility of the organization. C•CURE 9000 documentation may aid the organization in implementing this control.
PL-2	The organization: a. Develops a security plan for the information system that: - Is consistent with the organization's enterprise architecture; - Explicitly defines the authorization boundary for the system; - Describes the operational context of the information system in terms of missions and business processes; - Provides the security categorization of the information system including supporting rationale; -Describes the operational environment for the information system; -Describes relationships with or connections to other information systems; - Provides an overview of the security requirements for the system; - Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and - Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Reviews the security plan for the information system [Assignment: organization-defined frequency]; and c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.	**Not Applicable -** This control is the responsibility of the organization. C•CURE 9000 documentation may aid the organization in implementing this control.

Control	Requirement	C•CURE 9000
PL-4	The organization: a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.	**Not Applicable -** This control is the responsibility of the organization. C•CURE 9000 documentation may aid the organization in implementing this control.
PL-5	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.	**Not Applicable -** This control is the responsibility of the organization.
PL-6	The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.	**Not Applicable -** This control is the responsibility of the organization.
	PERSONNEL SECURITY	
PS-1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	**Not Applicable -** This control is the responsibility of the organization.
PS-2	The organization: a. Assigns a risk designation to all positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and revises position risk designations [Assignment: organization-defined frequency].	**Not Applicable -** This control is the responsibility of the organization.
PS-3	The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to [Assignment: organization-defined list of conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening].	**Not Applicable -** This control is the responsibility of the organization.

Control	Requirement	C•CURE 9000
PS-4	The organization, upon termination of individual employment: a. Terminates information system access; b. Conducts exit interviews; c. Retrieves all security-related organizational information system-related property; and d. Retains access to organizational information and information systems formerly controlled by terminated individual.	**Not Applicable -** This control is the responsibility of the organization.
PS-5	The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action].	**Not Applicable -** This control is the responsibility of the organization.
PS-6	The organization: a. Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access; and b. Reviews/updates the access agreements [Assignment: organization-defined frequency].	**Not Applicable -** This control is the responsibility of the organization.
PS-7	The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Documents personnel security requirements; and c. Monitors provider compliance.	**Not Applicable -** This control is the responsibility of the organization.
PS-8	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	**Not Applicable -** This control is the responsibility of the organization.
	RISK ASSESSMENT	
RA-1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	**Not Applicable -** This control is the responsibility of the organization.

Control	Requirement	C•CURE 9000
RA-2	The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	**Not Applicable -** This control is the responsibility of the organization.
RA-3	The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]]; c. Reviews risk assessment results [Assignment: organization-defined frequency]; and d. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, Tyco has performed an assessment of C•CURE 9000 against the applicable information assurance controls described in NIST SP 800-53.

Control	Requirement	C•CURE 9000
RA-5	The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for: -Enumerating platforms, software flaws, and improper configurations; -Formatting and making transparent, checklists and test procedures; and -Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).	**Compliant -** Responsibility for this control is shared by the organization and the system. In support of this control, Tyco performs a vulnerability scan on each release of C•CURE 9000 as part of its regulatory and compliance activity. Tyco also periodically engages a third-party information assurance consultant to perform independent vulnerability scan testing.
RA-5.1	The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.	**Compliant -** Responsibility for this control is shared by the organization and the system. In support of this control, Tyco performs a vulnerability scan using an industry standard tool on each release of C•CURE 9000 as part of its regulatory and compliance activity. Tyco also periodically engages a third-party information assurance consultant to perform independent vulnerability scan testing.
RA-5.2	The organization updates the list of information system vulnerabilities scanned [Assignment: organization-defined frequency] or when new vulnerabilities are identified and reported.	**Not Applicable -** This control is the responsibility of the organization.
RA-5.5	The organization includes privileged access authorization to [Assignment: organization-identified information system components] for selected vulnerability scanning activities to facilitate more thorough scanning.	**Not Applicable -** This control is the responsibility of the organization. C•CURE 9000 runs on an operating system that supports the implementation of this control.

Control	Requirement	C•CURE 9000
	SYSTEM AND SERVICES ACQUISITION	
SA-1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	**Not Applicable -** This control is the responsibility of the organization.
SA-2	The organization: a. Includes a determination of information security requirements for the information system in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.	**Not Applicable -** This control is the responsibility of the organization.
SA-3	The organization: a. Manages the information system using a system development life cycle methodology that includes information security considerations; b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and c. Identifies individuals having information system security roles and responsibilities.	**Not Applicable -** This control is the responsibility of the organization. C•CURE 9000 documentation may aid the organization in implementing this control.
SA-4	The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards: a. Security functional requirements/specifications; b. Security-related documentation requirements; and c. Developmental and evaluation-related assurance requirements.	**Not Applicable -** This control is the responsibility of the organization. C•CURE 9000 documentation may aid the organization in implementing this control.

Control	Requirement	C•CURE 9000
SA-4.1	The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.	**Compliant -** The C•CURE 9000 Cyber Security Hardening Guide provides the information described in this control.
SA-4.2	The organization requires in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls to be employed within the information system, information system components, or information system services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, Tyco can provide certain available design documentation upon request.
SA-4.3	The organization requires software vendors/manufacturers to demonstrate that their software development processes employ state-of-the-practice software and security engineering methods, quality control processes, and validation techniques to minimize flawed or malformed software.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, Tyco's software development processes are described within its process documents.

Control	Requirement	C•CURE 9000
SA-5	The organization: a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes: - Secure configuration, installation, and operation of the information system; - Effective use and maintenance of security features/functions; and - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and b. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes: - User-accessible security features/functions and how to effectively use those security features/functions; - Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and - User responsibilities in maintaining the security of the information and information system; and c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.	**Compliant -** Responsibility for this control is shared by the organization and the system. In support of this control, certain C•CURE 9000 documentation - including system manuals and guides - that responds to this control is available to the organization. The C•CURE 9000 Cyber Security Hardening Guide provides some of the information described in this control.
SA-5.1	The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.	**Compliant -** Responsibility for this control is shared by the organization and the system. In support of this control, the C•CURE 9000 Cyber Security Hardening Guide provides some of the information described in this control.
SA-5.2	The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing.	**Compliant -** Responsibility for this control is shared by the organization and the system. In support of this control, the C•CURE 9000 Cyber Security Hardening Guide and other system documentation provide some of the information described in this control.
SA-5.3	The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.	**Compliant -** Responsibility for this control is shared by the organization and the system. In support of this control, the C•CURE 9000 Cyber Security Hardening Guide and other system manuals, guides and proprietary documentation provide some of the information described in this control.

Control	Requirement	C•CURE 9000
SA-6	The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	**Not Applicable -** This control is the responsibility of the organization.
SA-6.1	The organization: a. Prohibits the use of binary or machine executable code from sources with limited or no warranty without accompanying source code; and b. Provides exceptions to the source code requirement only for compelling mission/operational requirements when no alternative solutions are available and with the express written consent of the authorizing official.	**Not Applicable -** This control is the responsibility of the organization.
SA-7	The organization enforces explicit rules governing the installation of software by users.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, Tyco provides release notes with each release to document any software limitations including installation.
SA-8	The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	**Not Applicable -** This control is the responsibility of the organization.
SA-9	The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Monitors security control compliance by external service providers.	**Not Applicable -** This control is the responsibility of the organization.

Control	Requirement	C•CURE 9000
SA-10	The organization requires that information system developers/integrators: a. Perform configuration management during information system design, development, implementation, and operation; b. Manage and control changes to the information system; c. Implement only organization-approved changes; d. Document approved changes to the information system; and e. Track security flaws and flaw resolution.	**Compliant -** The C•CURE 9000 development process includes processes, procedures and tools that implement this control.
SA-11	The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers): a. Create and implement a security test and evaluation plan; b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and c. Document the results of the security testing/evaluation and flaw remediation processes.	**Compliant -** The C•CURE 9000 development process includes processes, procedures and tools that implement this control.
	SYSTEM AND COMMUNICATIONS PROTECTION	
SC-1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	**Not Applicable -** This control is the responsibility of the organization.
SC-2	The information system separates user functionality (including user interface services) from information system management functionality.	**Compliant -** C•CURE 9000 provides three (3) account types - System Administrator, Personnel Administrator and Guard - that provide separation of user functionality. User account privilege assignments are configurable.

Control	Requirement	C•CURE 9000
SC-4	The information system prevents unauthorized and unintended information transfer via shared system resources.	**Compliant -** Responsibility for this control is shared by the organization and the system. C•CURE 9000 supports access by authenticated users that provide valid credentials assigned by the organization when accessing the system.
SC-5	The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list].	**Compliant -** Responsibility for this control is shared by the organization and the system. The host Windows operating system may provide policies and detection procedures for DOS attacks that are available to be configured by the organization. iSTAR controllers detect UDP DOS attacks and will temporarily shut down the communications port if a DOS situation is detected. Once proper connection is made with the server, this activity will be reported and written to Journal Database. In the case of a successful DOS attack, C•CURE 9000 can be configured to support two fail modes. Fail-secure mode allows for access to be locked during a failure of communication or power. Fail-safe mode unlocks access given the same conditions.
SC-7	The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	**Not Applicable -** This control is the responsibility of the organization.
SC-7.3	The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.	**Compliant -** Responsibility for this control is shared by the organization and the system. C•CURE 9000 documentation describes the access points for the system. The access points can be limited to those necessary to permit adequate functionality of the system.

Control	Requirement	C•CURE 9000
SC-7.4	The organization: a. Implements a managed interface for each external telecommunication service; b. Establishes a traffic flow policy for each managed interface; c. Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted; d. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; e. Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency]; and f. Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.	**Not Applicable -** This control is the responsibility of the organization.
SC-7.5	The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).	**Compliant -** Responsibility for this control is shared by the organization and the system. C•CURE 9000 documentation describes the access points for the system. The access points can be limited to those necessary to permit adequate functionality of the system.
SC-7.6	The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.	**Not Applicable -** This control is the responsibility of the organization.
SC-7.7	The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.	**Compliant -** Responsibility for this control is shared by the organization and the system. Access into the C•CURE 9000 console device is limited for remote access and the web portal allows for control over limited accesses. The organization's IT infrastructure is responsible for system connections to external networks.
SC-8	The information system protects the integrity of transmitted information.	**Compliant -** Responsibility for this control is shared by the organization and the system. C•CURE 9000 supports SSL connections for information transferred between remote user clients and C•CURE 9000. Information transferred between C•CURE 9000 and controllers can be configured for FIPS 140-2 encryption.

Control	Requirement	C•CURE 9000
SC-8.1	The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].	**Compliant -** Responsibility for this control is shared by the organization and the system. C•CURE 9000 supports SSL connections for information transferred between remote user clients and C•CURE 9000. Information transferred between C•CURE 9000 and controllers can be configured for FIPS 140-2 encryption.
SC-10	The information system terminates the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.	**Compliant -** C•CURE 9000 provides mechanisms that support this control.
SC-12	The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].	**Compliant -** Responsibility for this control is shared by the organization and the system. C•CURE 9000 supports the use of cryptographic keys. The organization is responsible for key management activities.
SC-13	The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	**Compliant -** C•CURE 9000 supports FIPS-140-2 compliant cryptography.
SC-13.4	The organization employs [Selection: FIPS-validated; NSA-approved] cryptography to implement digital signatures.	**Compliant -** C•CURE 9000 supports FIPS-140-2 compliant cryptography.
SC-15	The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and b. Provides an explicit indication of use to users physically present at the devices.	**Compliant -** C•CURE 9000 does not support collaborative computing devices.
SC-15.2	The information system or supporting environment blocks both inbound and outbound traffic between instant messaging clients that are independently configured by end users and external service providers.	**Not Applicable -** This control is the responsibility of the organization.
SC-16	The information system validates the integrity of security attributes exchanged between systems.	**Not Applicable -** This control is the responsibility of the organization.
SC-17	The organization issues public key certificates under an [Assignment: organization-defined certificate policy] or obtains public key certificates under an appropriate certificate policy from an approved service provider.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, C•CURE 9000 can employ certificates issued by an organization.

Control	Requirement	C•CURE 9000
SC-18	The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system.	**Compliant -** C•CURE 9000 does not host any type of "scripting" or code execution that can be transferred across systems. C•CURE 9000 is distributed as a standard MSI installation kit for Server and Client based PCs. This type of transfer is typically done on a DVD. There is a configurable "Client AutoUpdate" option. This is where the user configures the C-CURE 9000 Server with IIS (Internet Information Services), and clients can be scheduled to run and install software updates on the next client application instance.
SC-19	The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system.	**Not Applicable -** This control is the responsibility of the organization.
SC-20	The information system: a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent	**Compliant -** Responsibility for this control is shared by the organization and the system. C•CURE 9000 supports this control through the use of a DNS to resolve queries.
SC-21	The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.	**Compliant -** Responsibility for this control is shared by the organization and the system. C•CURE 9000 supports this control through the use of a DNS to resolve queries.
SC-22	The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.	**Not Applicable -** C•CURE 9000 does not provide a name/address resolution service.
SC-23	The information system provides mechanisms to protect the authenticity of communications sessions.	**Compliant -** C•CURE 9000 provides mechanisms that support this control.

Control	Requirement	C•CURE 9000
SC-24	The information system fails to a [Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures] preserving [Assignment: organization-defined system state information] in failure.	**Compliant -** C•CURE 9000 updates registry settings, files and databases in real time. When C•CURE 9000 is restarted after a failure, all settings are restored. Status is refreshed from controllers and other endpoints and clients. C•CURE 9000 documentation also describes troubleshooting steps for problems related to input/output, communications, licensing, startup and database restoration.
SC-28	The information system protects the confidentiality and integrity of information at rest.	**Not Applicable -** C•CURE 9000 is not an "at rest" data product.
SC-32	The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.	**Not Applicable -** This control is the responsibility of the organization. C•CURE 9000 may be deployed in a distributed environment. However, it is recommended to configure C•CURE 9000 components to operate within their own domain on a specific subnet to aid in securing and restricting access to the systems.
	SYSTEM AND INFORMATION INTEGRITY	
SI-1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	**Not Applicable -** This control is the responsibility of the organization.
SI-2	The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and c. Incorporates flaw remediation into the organizational configuration management process.	**Not Applicable -** This control is the responsibility of the organization. In support of this control, Tyco's flaw remediation process can correct system flaws and test the flaw solutions.

Control	Requirement	C•CURE 9000
SI-2.2	The organization employs automated mechanisms [Assignment: organization-defined frequency] to determine the state of information system components with regard to flaw remediation.	**Not Applicable -** This control is the responsibility of the organization.
SI-3	The organization: a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: - Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or - Inserted through the exploitation of information system vulnerabilities; b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: - Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and - [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.	**Not Applicable -** This control is the responsibility of the organization. Malicious code mechanisms are not provided with C•CURE 9000.
SI-3.1	The organization centrally manages malicious code protection mechanisms.	**Not Applicable -** This control is the responsibility of the organization. Malicious code mechanisms are not provided with C•CURE 9000.
SI-3.2	The information system automatically updates malicious code protection mechanisms (including signature definitions).	**Not Applicable -** This control is the responsibility of the organization. Malicious code mechanisms are not provided with C•CURE 9000.

Control	Requirement	C•CURE 9000
SI-4	The organization: a. Monitors events on the information system in accordance with [Assignment: organization-defined monitoring objectives] and detects information system attacks; b. Identifies unauthorized use of the information system; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.	**Not Applicable -** This control is the responsibility of the organization.
SI-4.2	The organization employs automated tools to support near real-time analysis of events.	**Not Applicable -** This control is the responsibility of the organization. Audit logging functionality exists in C•CURE 9000 to support SI-4 and this SI-4 control enhancement.
SI-4.4	The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.	**Not Applicable -** This control is the responsibility of the organization. Audit logging functionality exists in C•CURE 9000 to support SI-4 and this SI-4 control enhancement.
SI-4.5	The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: [Assignment: organization-defined list of compromise indicators].	**Not Applicable -** This control is the responsibility of the organization. Audit logging functionality exists in C•CURE 9000 to support SI-4 and this SI-4 control enhancement.
SI-4.6	The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.	**Not Applicable -** This control is the responsibility of the organization. Audit logging functionality exists in C•CURE 9000 to support SI-4 and this SI-4 control enhancement.

Control	Requirement	C•CURE 9000
SI-4.10	The organization makes provisions so that encrypted traffic is visible to information system monitoring tools.	**Not Applicable -** This control is the responsibility of the organization.
SI-4.12	The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [Assignment: organization-defined list of inappropriate or unusual activities that trigger alerts].	**Not Applicable -** This control is the responsibility of the organization.
SI-5	The organization: a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to [Assignment: organization-defined list of personnel (identified by name and/or by role)]; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	**Not Applicable -** This control is the responsibility of the organization. Tyco can support response and remediation related to security alerts, advisories and directives.
SI-5.1	The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.	**Not Applicable -** This control is the responsibility of the organization. Tyco can support response and remediation related to security alerts, advisories and directives.
SI-7	The information system detects unauthorized changes to software and information.	**Compliant -** Responsibility for this control is shared by the organization and the system. C•CURE 9000 and the host OS/platform allow only users with valid authenticated credentials to input information to the system.
SI-7.1	The organization reassesses the integrity of software and information by performing [Assignment: organization-defined frequency] integrity scans of the information system.	**Not Applicable -** This control is the responsibility of the organization.

Control	Requirement	C•CURE 9000
SI-8	The organization: a. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.	**Not Applicable -** This control is the responsibility of the organization.
SI-8.1	The organization centrally manages spam protection mechanisms.	**Not Applicable -** This control is the responsibility of the organization.
SI-9	The organization restricts the capability to input information to the information system to authorized personnel.	**Compliant -** Responsibility for this control is shared by the organization and the system. C•CURE 9000 only allows users with valid authenticated credentials to input information to the system.
SI-10	The information system checks the validity of information inputs.	**Compliant -** C•CURE 9000 performs validation testing on information inputs.

Control	Requirement	C•CURE 9000
SI-11	The information system: a. Identifies potentially security-relevant error conditions; b. Generates error messages that provide information necessary for corrective actions without revealing [Assignment: organization-defined sensitive or potentially harmful information] in error logs and administrative messages that could be exploited by adversaries; and c. Reveals error messages only to authorized personnel.	**Compliant -** Responsibility for this control is shared by the organization and the system. The organization has primary responsibility for identifying the potentially security-relevant error conditions. C•CURE 9000 supports this control by reporting server failures, controller failures, controller connection status, database backup failures, C•CURE 9000 provides the ability to configure log messages associated with these conditions. Windows OS errors (e.g., service, connections) are written to Windows event logs. The C•CURE 9000 server also has configurable “tracing” that is turned off by default. Turning these options on are part of the server management application. Several different tracing types can be turned on or off. Once turned on, the system writes to multiple trace files that are stored on the server. Pre-defined and customizable messages can be used to provide corrective action information. Error messages do not display excessive information. These messages are only available to operators who have appropriately configured privileges.
SI-12	The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	**Not Applicable -** This control is the responsibility of the organization.