

The Infor logo consists of the word "infor" in a white, lowercase, sans-serif font, centered within a solid red square. A small trademark symbol (TM) is located to the right of the red square.

infor™

APRIL 2020

# INFOR REGULATED INDUSTRIES SAAS

Infor user guide to support compliance with North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards

# Contents

---

Notices .....	<b>03</b>	Solution alignment with NERC and NIST CSF .....	<b>14</b>
About this guide .....	<b>04</b>	CSF core functions .....	<b>15</b>
Overview .....	<b>04</b>	Identity and access management .....	<b>16</b>
Background .....	<b>04</b>	Data protection .....	<b>17</b>
Infor alignment with utilities operational and compliance needs .....	<b>05</b>	Patching and vulnerability management .....	<b>17</b>
Security assurance programs and inheriting controls .....	<b>05</b>	Security event monitoring .....	<b>19</b>
Security and shared responsibility .....	<b>07</b>	Incident response .....	<b>20</b>
Security TO the cloud .....	<b>08</b>	Resilience and system recovery .....	<b>20</b>
Security IN the cloud .....	<b>09</b>	Physical security .....	<b>20</b>
Security OF the cloud .....	<b>09</b>	Planning considerations for use of cloud services .....	<b>21</b>
Shared Responsibility and Applicable Services by Standard .....	<b>10</b>	Contributors .....	<b>21</b>
Implementing controls to support security and compliance objectives .....	<b>10</b>	Additional Resources .....	<b>21</b>
		Appendix: Infor solutions and services and alignment to NERC CIP .....	<b>22</b>

# Notices

---

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current Infor product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from Infor and its affiliates, suppliers or licensors. Infor products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of Infor to its customers are controlled by Infor agreements, and this document is not part of, nor does it modify, any agreement between Infor and its customers.

© 2020 Infor. All rights reserved.

## About this guide

This document describes how customers can use Infor services to realize the benefits of cloud technology and meet compliance requirements for the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards. This document explains core cloud security concepts as they apply to NERC CIP objectives, demonstrates how Infor services align to the NERC CIP requirements, and discusses how NERC Responsible Entities can plan their migration to the Infor Cloud.

## Overview

This User Guide demonstrates how Infor provides a secure and reliable infrastructure, and how the wide range of Infor Cloud solutions can be used to meet the security and reliability objectives of the NERC CIP standards. The following sections provide information on Infor products and services that enable customers to meet and sustain compliance with NERC CIP standards, how these services align with the NERC CIP standards, and considerations for customers as they plan use of Infor Cloud solutions for data and systems within the regulated scope.

## Background

Infor recognizes that our Power and Utility customers are interested in leveraging cloud computing technology to meet their business objectives and the needs of their customers. **IDC noted:**

“As the power and utility sector increases its digital capabilities, cloud offerings and services present companies with an attractive option for lowering overall IT and infrastructure costs while providing scalable and secure data storage with on-demand access.”

As technology evolves in areas such as virtualization and cloud computing, entities, regulators, and service providers are engaging to enable use of new technology and to enable Responsible Entities to meet their operational, security, and resiliency objectives.

The US electric sector is regulated by the Federal Energy Regulatory Commission (FERC), a federal independent agency that regulates the interstate transmission of liquefied natural gas, oil, and electricity, along with natural gas and hydropower projects. US electric sector entities are subject to mandatory and enforceable security requirements to protect the reliability of the Bulk Electric System (BES).

In 2006, FERC certified the North American Electric Reliability Corporation (NERC) as the Electric Reliability Organization with authority to develop Critical Infrastructure Protection (CIP) cybersecurity reliability standards, which are written to ensure the security and reliability of grid planning and operations. Entities with assets that meet the defined criteria are mandated to comply with the NERC CIP standards for the data, assets, and systems in-scope of the standards.

To encourage discussion, FERC held panels at Reliability Technical Conferences to discuss how standards can evolve to best leverage the benefits of a cloud environment effectively and securely for utility planning and operations. Existing CIP drafting teams are following the Standards Development Process to assess and propose language revisions, where appropriate.

### **FERC Staff report, FERC Commission Open Meeting, November 21, 2019**

Cloud/Managed Security Service Provider: This focus area acknowledges that as entities explore how to deploy cloud and managed security service providers, it is critical that they do so in a secure manner. If implemented properly, the use of a trusted third party to perform common tasks and services can yield security benefits by allowing the entity to focus on more complex issues in house and to optimize their security resources. However, more research needs to be conducted to determine if the most critical systems, such as those used for real-time operations, could be used in the cloud.

Technical stakeholder working groups are evaluating the use of cloud services relative to the requirement language and evidence obligations and writing guidance to address how Responsible Entities can demonstrate compliance with the CIP standards when using cloud services. Specifically, guidance is being drafted for protection of BES Cyber System Information (BCSI) in the cloud. In June 2019, NERC endorsed guidance to rely on a third party's independent assessment as an acceptable means of identifying and assessing risk. (See [NATF CIP-013-1 Implementation Guidance](#)).

## **Infor alignment with utilities operational and compliance needs**

Infor believes that the utility industry is undergoing a massive transformation, similar to what is occurring in many other industries. New business models, different market dynamics, increased customer expectations, and emerging technologies are pushing traditional utility business models in different directions sooner and faster than ever before. The pace of change is creating challenges for utilities to keep up in every area that they typically serve, including generation, transmission & distribution, renewables, and the expectation is that this pace of change will continue to affect the utility industry significantly over the next 10 years and beyond.

One of the main challenges that utilities are facing is being asked to do more with their assets than ever before while continuing to try and reduce the cost of maintaining them. The different business models have forced assets into different operating scenarios, and many times into scenarios for which they were not designed. Power generators are being forced into different duty cycles, while transmission and distribution assets are being tasked with carrying more load into more areas more frequently than ever before. The stress on the infrastructure and the people that maintain it is at an all-time high. The need to be able to gather data from the assets within the system and make that data work for the benefit of the organization and the people that maintain it has become critical and cost control has become more important than ever.

Infor believes that we are well-positioned to help utilities address the challenges they are facing, like asset management, and take advantage of the opportunities that will be created over the next 5 to 10 years and beyond. We work with utilities all over the world to provide asset management solutions in power generation, transmission, and distribution, and we understand what it takes to manage these assets in the most efficient and cost-effective manner possible. Infor CloudSuite solutions have been designed with the flexibility and functionality necessary to meet the current changing needs of the utility industry and into the future.

## **Security assurance programs and inheriting controls**

Infor aligns with other security assurance programs that evaluate, assess, and monitor cyber security controls on network infrastructure, applications, and services to comport with requirements of existing US government programs. These security assurance programs are consistent with the CIP security objectives. Customers can help meet the CIP security objectives for cloud SaaS through inherited controls managed by Infor and AWS by leveraging tools that empower users to secure their cloud environments.

Infor and AWS maintain certifications and independent, third-party attestations for a variety of industry specific workloads. Infor is routinely audited for its compliance to these assurance programs, which includes continuous monitoring.

Customers can leverage Infor and AWS assurance reports to help demonstrate compliance for security of the cloud, in addition to their own complementary controls that detail their unique and specific configurations and demonstrate their compliance for security of their resources in the cloud.

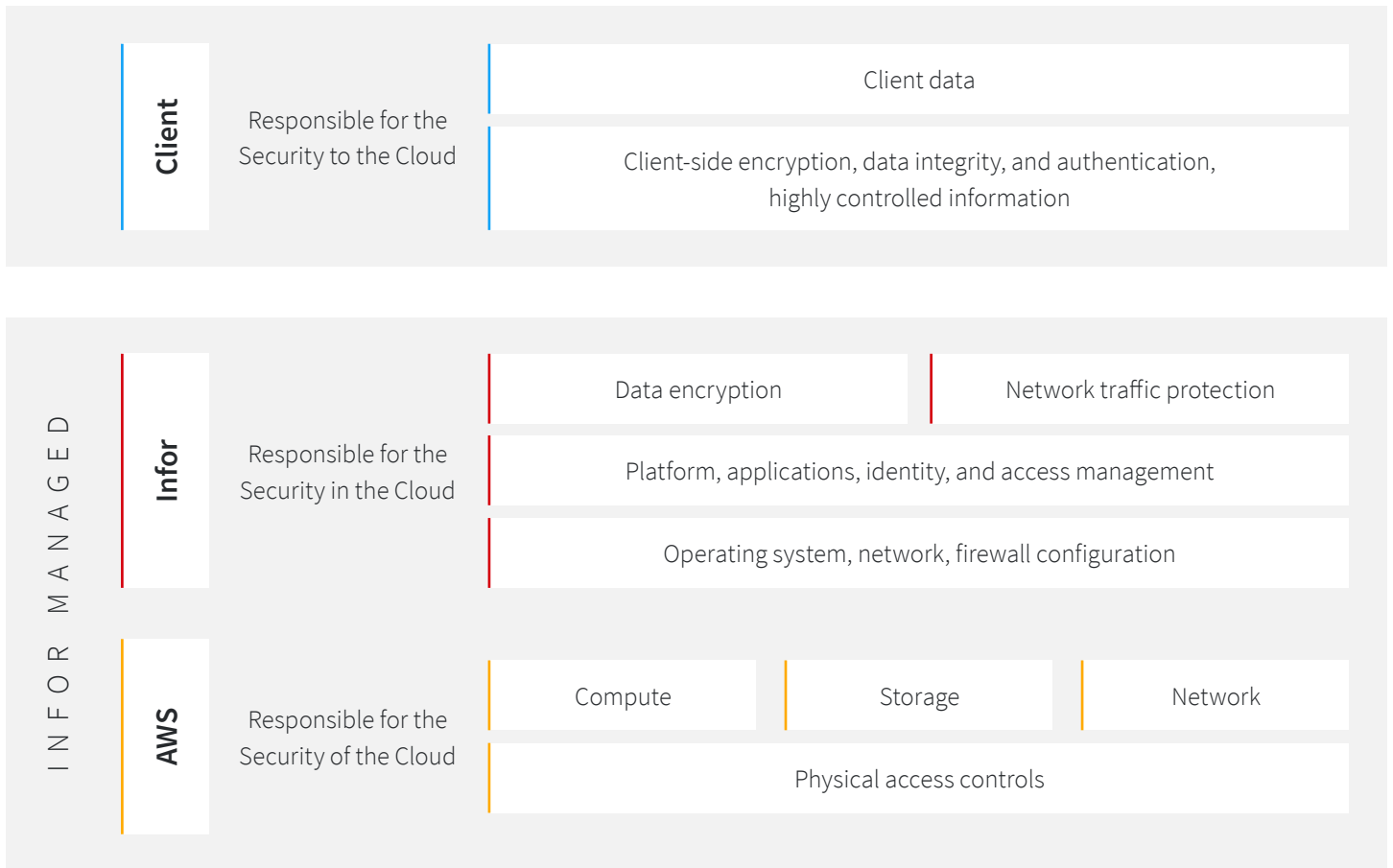
Some of the assurance programs of particular interest to NERC regulated entities are:

FRAMEWORK	COMPLIANCE AREAS
<b>National Institute of Standards and Technology (NIST) Cybersecurity</b>	<p>The CSF can serve as the common ground to meet security and compliance objectives for the entire organization. Many technology providers have already mapped their services and products to the NIST CSF, thereby streamlining assessments, acquisition, and compliance, and at a lower cost. For more information about NIST CSF, including the full definition of the security control baselines, visit the <a href="#">NIST CSF</a> webpage.</p>
<b>Federal Risk Assessment and Management Program (FedRAMP)</b>	<p>Provides a standardized assessment and authorization process for cloud service providers (CSPs) and uses NIST CSF, primarily NIST 800-53 controls along with Federal Information Processing Standards (FIPS). A provisional authorization from FedRAMP provides a reusable certification that attests to compliance reducing the time necessary for a Government mission owner to assess and authorize one of their systems for operation. Aligned with DoD CC SRG. For more information about FedRAMP, including the full definition of the security control baselines, visit the <a href="#">FedRAMP</a> webpage.</p>
<b>DoD Cloud Computing System Reference Guide (SRG)</b>	<p>Provides a standardized assessment and authorization process for CSPs to gain a DoD provisional authorization, so that they can serve DoD customers. A provisional authorization from the Defense Information Systems Agency (DISA) provides a reusable certification that attests to compliance with DoD standards, reducing the time necessary for a DoD mission owner to assess and authorize one of their systems for operation. For more information about the SRG, including the full definition of the security control baselines, visit the <a href="#">Document Library</a> on the <a href="#">DoD Cloud Computing Security</a> webpage. Aligned with NIST CSF and FedRAMP.</p>
<b>Health Insurance Portability and Accountability Act of 1996 (HIPAA)</b>	<p>HIPAA required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. To fulfill this requirement, HHS published what are commonly known as the HIPAA <a href="#">Privacy Rule</a> and the HIPAA <a href="#">Security Rule</a>. For more information about HIPAA, including the full definition of the security control baselines, visit the <a href="#">HIPAA</a> and the <a href="#">HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework</a> webpages.</p>
<b>Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting (ICFR)</b>	<p>These reports, prepared in accordance with AT-C section 320, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting, are specifically intended to meet the needs of entities that use service organizations (user entities) and the CPAs that audit the user entities' financial statements (user auditors), in evaluating the effect of the controls at the service organization on the user entities' financial statements.</p>

## Security and shared responsibility

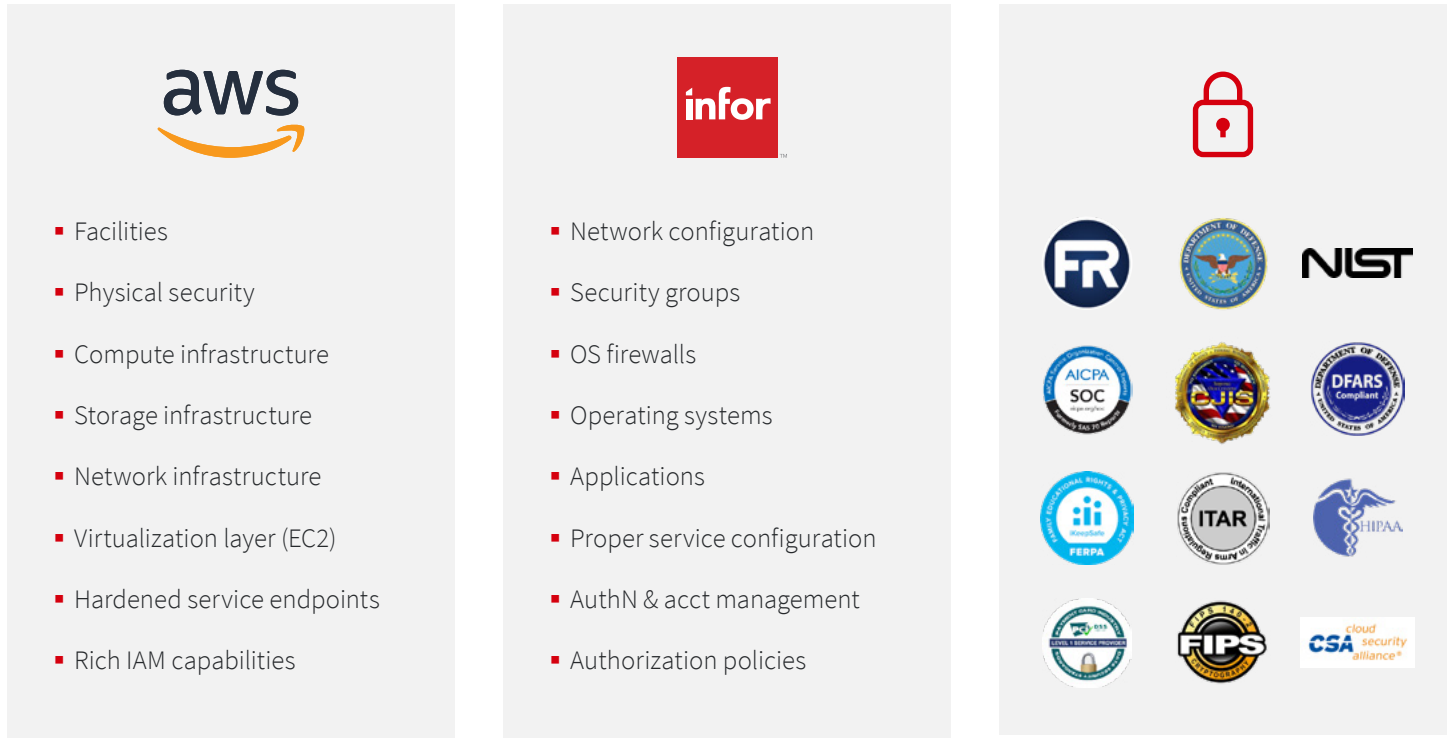
Cloud security is a shared responsibility. The **Shared Responsibility Model** is fundamental to understanding the respective roles of the customer and Infor in the context of the cloud security principles (Figure 1). Infor manages security of Infor cloud offering by ensuring that Infor SaaS complies with global and regional regulatory requirements and best practices. Infor has partnered with AWS to provide security of the cloud. The customer is the responsible for security to the cloud to meet their policies, procedures, and regulatory requirements. This means that customers retain control of the security program they choose to implement to protect their own content.

**Figure 1: Shared responsibility model**



Infor has partnered with AWS to operate, manage, and control the IT components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate (Figure 2).

**Figure 2: Infor and AWS responsibilities**



Customers get to choose the right level of security for their business.  
As a cloud customer you can focus on your business.

In fulfilling CIP compliance, NERC Responsible Entities are responsible for ensuring compliance with NERC CIP requirements; however, fulfillment of the controls depends on the applicable IT component. Responsible Entities manage controls for NERC CIP classified assets; Infor manages the security in the cloud and AWS manages controls for the cloud infrastructure; and all Responsible Entities perform security control activities for requirements that apply to the SaaS, including cloud infrastructure and NERC CIP classified assets.

### Security TO the cloud

Customers are responsible for security to the cloud. Responsibility includes client data, client-side encryption, data integrity, user authentication, and who has access to their content and how those access rights are granted, managed, and revoked. This means that customers retain control of the security program they choose to implement to protect their own content.

Infor customers in scope for NERC CIP are responsible for managing controls to ensure security to the cloud. Some NERC CIP requirements are addressed by entity specific policies, plans or processes managed by the Responsible



Entity, among them the asset classification process of CIP-002; the overarching policies required in CIP-003; and the incident response plans of CIP-008. Whereas cloud services may be used to support performance of these controls, customers will follow their compliance program to meet these requirements and should update governing documents that may be appropriate to accommodate cloud services.

## Security IN the cloud

Infor is responsible for security in the cloud. Infor is responsible for managing the operating systems (including installing updates and security patches) and other associated application software, as well as the configuration of the security group firewall. Infor carefully considers the services they chosen, as responsibilities vary depending on the services they use, the integration of those services into SaaS environments, and applicable laws and regulations.

When using Infor solutions, Infor maintains control over the systems within the cloud and is responsible for managing the configuration of the security controls, including:

- High availability and disaster recovery
- Resilience of architecture to ensure availability
- Change management and incident management
- AWS services and security features that are used
- The country where their content is stored
- How their data is encrypted and where the keys are stored

## Security OF the cloud

To provide security of the cloud, AWS environments are continuously audited, and the infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and verticals. Infor uses these certifications to validate the implementation and effectiveness of AWS security controls, including internationally recognized security best practices and certifications. The AWS compliance program is based on the following actions:

### Validate

- AWS services and facilities across the globe maintain a ubiquitous control environment that is operating effectively.
- AWS control environment includes policies, processes, and control activities that leverage various aspects of the AWS overall control environment.
- The collective control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of our control framework.
- AWS has integrated applicable cloud- specific controls identified by leading cloud computing industry bodies into the AWS control framework.
- AWS monitors these industry groups to identify leading practices that Infor has implemented, and to better assist with managing Infor's control environment.

## **Demonstrate**

- AWS compliance posture to help Infor verify compliance with industry and government requirements.
- AWS engages with external certifying bodies and independent auditors to provide customers with considerable information regarding the policies, processes, and controls established and operated by AWS.
- Infor leverages this information to perform control evaluation and verification procedures, as required under the applicable compliance standard.

## **Monitor**

- AWS provides a safe and secure environment and empowers Infor to secure its infrastructure through the use of thousands of security control requirements.

Customers inherit the controls that provide security of the cloud infrastructure through Infor's Authorizations and Attestations.

## **Shared Responsibility and Applicable Services by Standard**

Appendix: Infor Services and Alignment to NERC CIP includes a table that offers more details on the shared responsibilities and inherited controls, and illustrates how they apply by CIP standard and requirement.

## **Implementing controls to support security and compliance objectives**

Dealing with the multitude of regulations across numerous industries is daunting for many organizations. The industries most affected are the financial, retail and e-commerce, health insurance and services, other insurance institutions, banking, defense, utilities, and credit card issuers who have access to sensitive information. But the list also includes any organization that keeps sensitive information—for example—any organization that has social security numbers; this encompasses most employers, government entities, and colleges and universities.

Compliance is a complicated, ever-evolving practice that requires a reliable, adaptable framework. You must not only create a secure storage system for sensitive data, but also act defensively in the event of potential security breaches. When choosing a system to accommodate your compliance needs, look for solutions that ensure confidentiality, integrity, reliability, or availability of information—chances are there are numerous regulations that demand compliance.

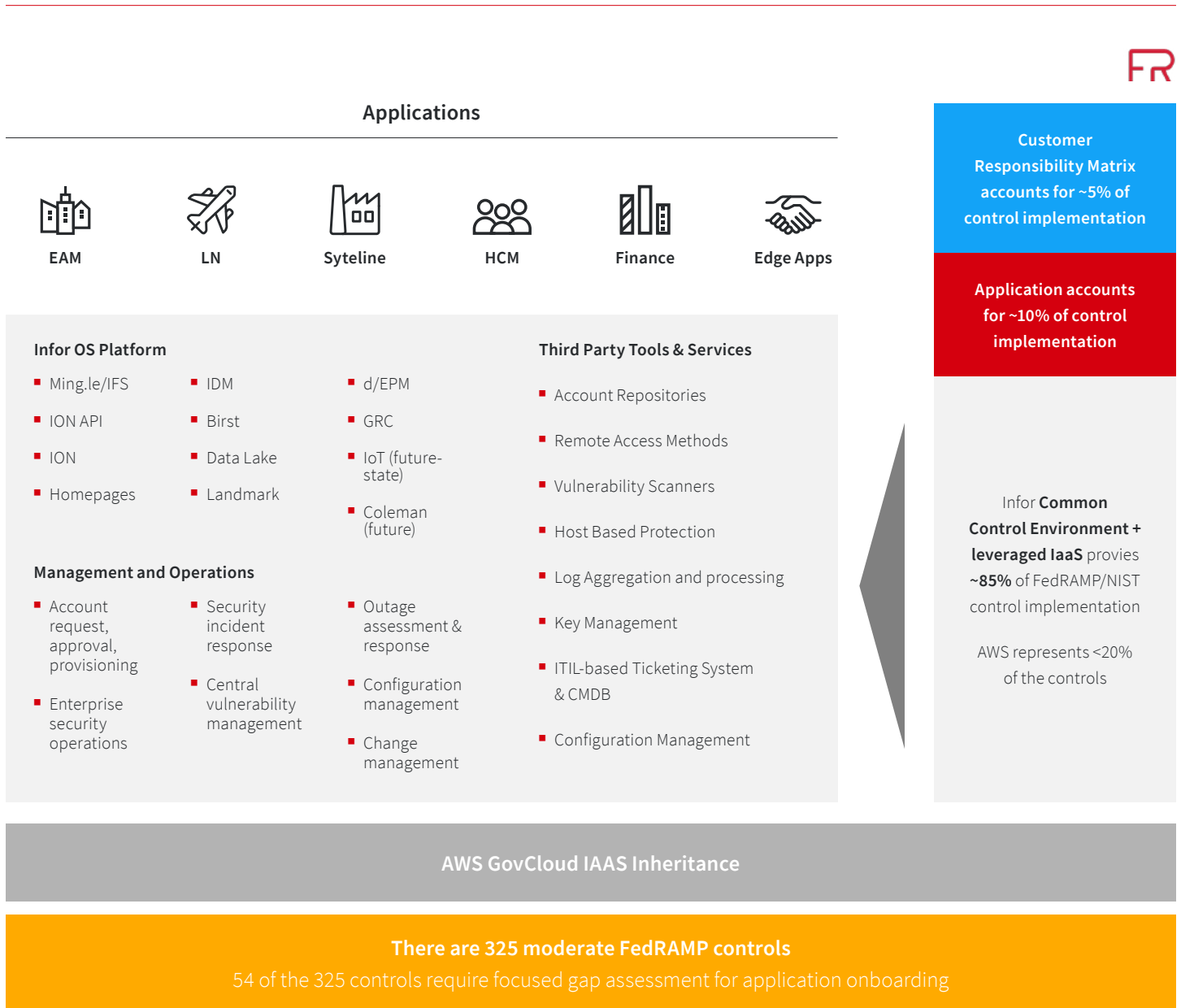
### **Infor's FedRAMP and NIST approach delivers inheritable security posture**

FedRAMP and NIST Cybersecurity Framework allows for inherited controls and stacking of authorization packages like building blocks. Infor CloudSuite solutions are also architected to inherit capabilities, including security controls, from a common technology platform (Infor OS). CloudSuites consist of Infor application bundles that follow enterprise policies and processes as well as:

- Software development standards for all Infor products
- Standard operating procedures for Infor cloud operations
- Capabilities based on “defense-in-depth” principles
- Reference architectures and certified integrations

Infor's CloudSuite compliance approach combined with FedRAMP and NIST means that customers can adopt and deploy secure cloud solutions more quickly. Inherent security and compliance features of the cloud enable customers to meet their security objectives (Figure 3).

**Figure 3: Infor compliance approach**


**AWS GovCloud IAAS Inheritance**
**There are 325 moderate FedRAMP controls**  
 54 of the 325 controls require focused gap assessment for application onboarding
 

Infor CloudSuite architecture is designed to provide enhanced security and reliability that includes:

### Infor cloud platform

Infor's cloud platform brings business processes, commerce network, business analytics, and artificial intelligence together. The platform is designed to deliver technology that drives business and mission outcomes, putting the customer at the center of every experience.

**Infor Operating Service (Infor OS)** provides cloud computing architecture and in-memory computing technology that delivers high performance, support for open standards, enhanced productivity, responsive design, and mobile access via a wide range of devices. The various components of the Infor OS platform work together to automate, anticipate, predict, and inform stakeholders, unifying the customer experience to support the mission.

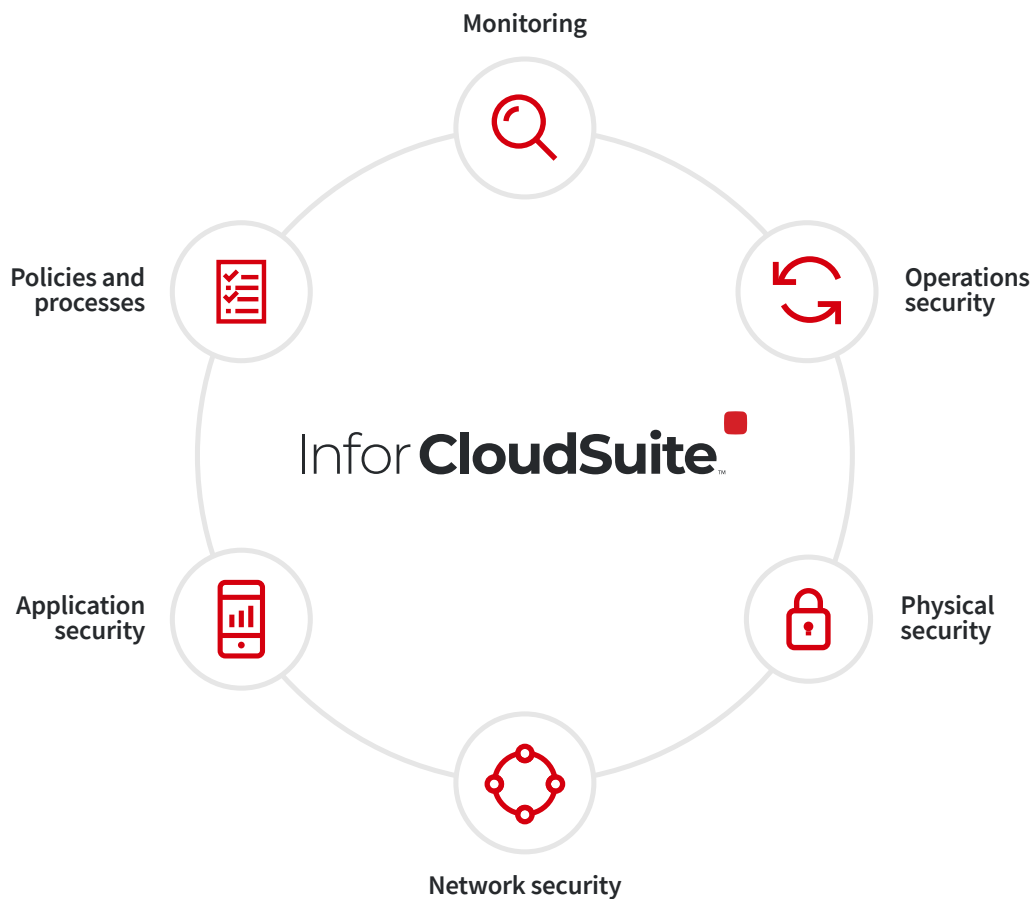
## Infor industry CloudSuites

Built-in industry expertise means that Infor CloudSuite solutions can be implemented with configuration, not customization. Plus, all the resources and equipment needed to get up and running are handled by Infor’s partner, Amazon® Web Services (AWS®). This enables much faster implementation time than with typical on-premises solutions.

Infor OS provides your cloud operating platform for the future and delivers technology that goes beyond enabling business—it drives it, putting the user at the center of every experience, and serving as a unifying foundation for your entire business ecosystem. The result is a connected, intelligent network that automates, anticipates, predicts, and informs your stakeholders, unifying your business.

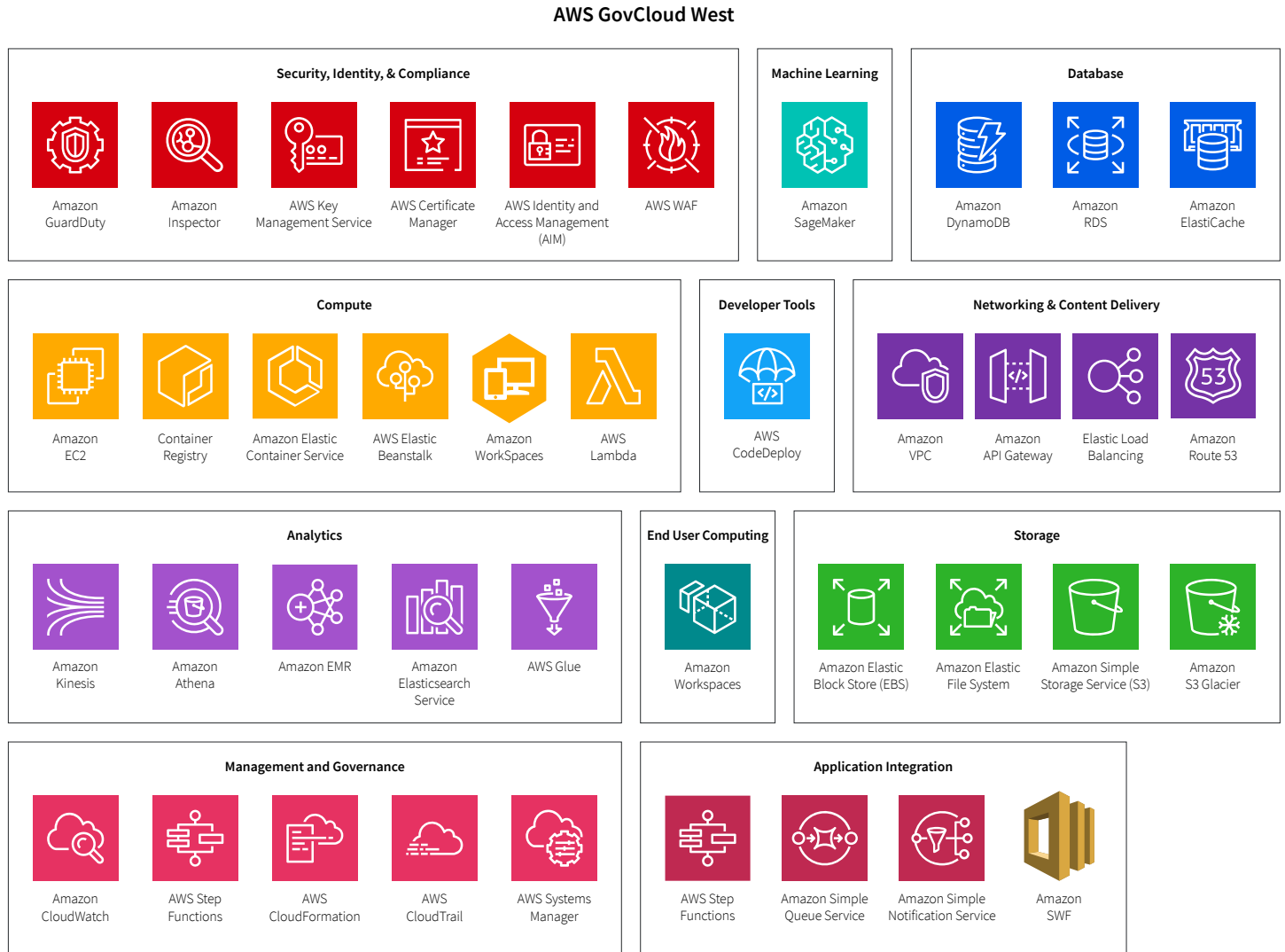
Infor CloudSuite does not rely on any single security device, technique, or practice for data assurance. Instead, Infor CloudSuite employs a “defense-in-depth” strategy (Figure 4) to implement multiple layers of overlapping security that safeguard your data through each link of the chain and ensure a high level of solution availability. These security controls are enforced by a team of specialists who are constantly monitoring and improving our security posture to stay ahead of threats.

**Figure 4. CloudSuite defense in depth**



Infor simplifies compliance auditing, security analysis, change management, and operational troubleshooting by using the following AWS services (Figure 5):

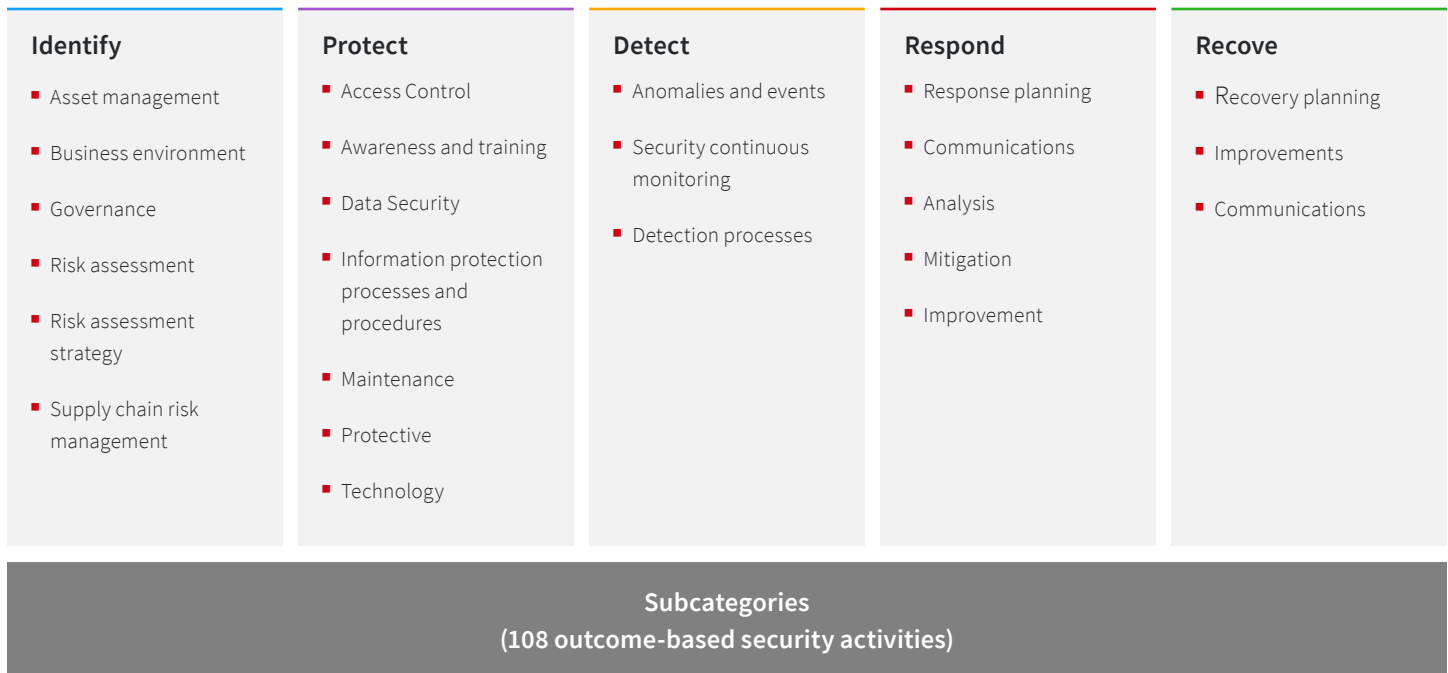
**Figure 5: IRIS AWS GovCloud services used**



## Solution alignment with NERC and NIST CSF

The following sections show how customers using IRIS CloudSuites fulfill the security objectives addressed in the NERC CIP standards.

**Figure 6. NIST CSF functions and categories**





The subcategories describe expected outcomes of a cybersecurity program. Each subcategory is matched with relevant Informative References.

## CSF core functions

Infor Security Incident Response Process (SIRP) leverages NIST 800-61 guidance, industrial best practices such as ITIL, and the model is designed to comply CSF Core Functions and meet FedRAMP control implementation requirements, as well as other applicable laws, regulations, and standards. The sub-processes documented within the main process domains (Figure 7) below serve as the underpinnings for the FedRAMP Incident Response family control implementation as outlined below.

**Figure 7. Infor Security Incident Response Process leverages NIST CSF**

---

			
<ul style="list-style-type: none"><li>▪ Preparing to handle incidents</li><li>▪ Preventing incidents</li></ul>	<ul style="list-style-type: none"><li>▪ Attack vectors</li><li>▪ Signs of an incident</li><li>▪ Sources of precursors and indicators</li><li>▪ Incident analysis</li><li>▪ Incident documentation</li><li>▪ Incident prioritization</li><li>▪ Incident notification</li></ul>	<ul style="list-style-type: none"><li>▪ Choosing a containment strategy</li><li>▪ Evidence gathering and handling</li><li>▪ Identifying the attacking hosts</li><li>▪ Eradication and recovery</li></ul>	<ul style="list-style-type: none"><li>▪ Lessons learned</li><li>▪ Using collected incident data</li><li>▪ Evidence retention</li><li>▪ Incident handling checklist</li></ul>

The following sections show how customers using IRIS CloudSuites fulfill the security objectives addressed in the NERC CIP standards.

## Identity and access management

CIP-004 thru CIP-007 includes requirements around access authorization, monitoring, audit, and revocation. In the cloud, these requirements can be addressed by managing access to perform cloud configuration and management activities; remote access to servers in the cloud; and end user access to applications. Infor uses several tools and services to manage users in all these categories.

Infor “Security Policy” directs the activities within the Infor Regulated Industries SaaS (IRIS) Identity and Access Management (IAM) procedure. The plan addresses purpose, scope, responsibilities (including management commitment), coordination among organizational entities, and compliance requirements to meet the FedRAMP and NIST control implementation requirements for the access control family of a moderate baseline. The Access Management Plan addresses topics related to:

- Information Access Restriction
- The Request Fulfillment Process for Provisioning GovCloud Access
- Managing the Administrative privileges
- The Periodic Review of GovCloud Access
- The Revocation of GovCloud Access
- The Separation of Duties
- Password Policy
- Access Control to Program Source Code
- Authenticator Device Management

Infor policies and procedures are captured in Infor’s document repository management system and reviewed within FedRAMP requirements by the document owner.

**Customer IAM:** Customer provided identity management solutions will be used by IRIS to allow customer user access via Security Assertion Markup Language (SAML) assertions. Groups, roles, and access authorization rights in IRIS applications are configurable by the customer. It is a customer responsibility to create or customize IRIS application groups, roles, and access authorization rights appropriate for their organization, approve access authorizations including group membership and assign users to IRIS application groups.

**Infor Privileged User IAM:** The personnel roles and privileges documented in the Roles and Responsibility Guide (RRG) that correspond to the mission/business functions of the CloudOps and SecOps teams that support the IRIS environment:

- CloudOps Team–Comprised of network, database, and system administrators that manage the overall operation of IRIS infrastructure and applications with system roles, details provided in RRG.
- SecOps Team–Comprised of Security Analysts with system roles, details provided in RRG.
- Infor conducts periodic access reviews on an annual basis, such that:
  - The Infor Security Office is responsible for leading the annual review of IRIS access.
  - CloudOps managers must participate in the annual review process and supply information as needed.
  - The Infor Security Office documents the results in Incident Management Tracking System (IMTS) and ensures access is removed from individuals no longer requiring access or specific privileges.



## Data protection

Customers can meet their requirements for protecting data throughout the lifecycle, for data at-rest, in-transit and in-use (CIP011-2, Information Protection). Customers retain ownership and control of their content along with the ability to encrypt it, protect it, move it, and delete it in alignment with their organization's security policies.

Infor manages the periodic backup and redundancy of Customer Data, product configurations, and product installations for Subscription Services. All Infor-initiated Subscription Service backups are exclusively for data recovery in the event of data loss. Backups of applicable Customer Data are retained for no less than thirty (30) calendar days.

Infor Cloud Services and IRIS must use Federal Information Processing Standard (FIPS) validated or National Security Agency (NSA) approved cryptographs in accordance with applicable federal laws, Executive Orders, directives, policies, regulation, and standards. Infor cloud environments and applications outside of IRIS that are not currently using FIPS-validated or NSA-approved cryptographs must have an approved exception from the ISO and a plan for migrating to FIPS-validated or NSA-approved cryptographs. Applications onboarding into IGS must document their approved encryption and key management scheme as a separate appendix to this document. All applications and environments must use FIPS compliant ciphers and hashes.

For infrastructure, Infor's partner AWS follows standards to install, service, and eventually destroys the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in **NIST 800-88**. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.

## Patching and vulnerability management

Customers can address their security objectives for patching and malicious code protection (CIP-007, Systems Security Management), and configuration and vulnerability management (CIP-010, Configuration Change Management and Vulnerability Assessment) inheriting Infor's FedRAMP and NIST controls for Patch and Vulnerability Management.

**Patch Management:** Infor, like many SaaS-focused organizations, is moving to a versionless software solution. New functionality and updates are released monthly, as needed. Infor manages upgrading environments to the current version of the Subscription Software. Infor follows ITIL and NIST standards for change management and will provide notifications and release notes for any changes to the applications, per the terms of our SLA.

Products that are Fixed/Patched in place for all customers on the same instance at the same time. Customers can however choose a time for their upgrade up to the time that an older version is retired. Version retirements are announced at least 9 months in advance. Customers still on a version being retired will be provided with an Upgrade date at least 60 days prior to the upgrade date.

Because application of the Fixes/Patches/Upgrades affects multiple Infor customers, an individual Licensee will not be able to delay, forego, or opt out of the date and time when the Fixes/Patches/Upgrades are scheduled to be applied.

Fixes/Patches/Upgrades are deployed to all customers and all customer environments (production, test, etc.) on the same instance at the same time, as there is only a single code-set shared by all tenants on a given instance.

**Vulnerability management:** Infor Global Policies directs the activities within security monitoring and vulnerability management documents. These documents address purpose, scope, responsibilities (including management commitment), coordination among organizational entities, and compliance requirements to meet the FedRAMP and NIST control implementation requirements for the access management control family of a moderate baseline. The plan specifically addresses procedures or processes related to:

- Vulnerability Management & Continuous Monitoring
- Vulnerability Scanning Tool Work Instructions
- Critical Milestones and Service Level Agreements
- Security Monitoring
- Vulnerability Remediation

Infor conducts assessments 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 based on the Infor Risk Management Framework, which was constructed in accordance the National Institute of Standards and Technology (NIST) SP 800-39 and the risk assessment process as detailed in NIST SP 800-30.

Infor has implemented a continuous monitoring strategy to support its FedRAMP and other regulatory compliance requirements. The strategy requires that Infor risk assessments take place annually, or more frequently as circumstances necessitate. The risk assessments illustrate the effectiveness of existing information security controls and safeguards, as well as the identity of new risks.

These assessments ensure all policies and supporting procedures properly address the boundary authorization in accordance with changing regulatory, contractual, business, technical, and operational requirements.

Infor conducts monthly web app, OS and DB scans and perform the vulnerability analysis needed to produce the FedRAMP monthly deliverables.

## Security event monitoring

CIP007, Systems Security Management, includes requirements for security event monitoring. Infor's SaaS System Event Log and Alert Management document provides direction for enhancing Infor Regulated Industries SaaS (IRIS) and Commercial SaaS system security and integrity through logging and auditing automation.

The customer is responsible for all customer application data, including the people, places, things, business rules, and events in relation to the customer's business goals/mission. Auditable events regarding customer application data can be captured to support the customer and made accessible to customers through the application.

As part of FedRAMP control, AU-2c, Infor has determined that customer application data events are not required to support after the fact investigations of security incidents and will not be in scope for FedRAMP's AU controls. Selected audit events will not include customer application data events that are defined as the customer's responsibility above.

The following sources of audit events are important for maintaining security of our environments:

EVENT SOURCE	DESCRIPTION
<b>Infor SaaS Applications</b>	Proprietary software
<b>Infor CloudSuite Portal (CSP)</b>	Proprietary software
<b>Web Servers</b>	Web access logs on servers and AWS Load Balancers
<b>AWS CloudTrail</b>	Captures all changes to AWS resources
<b>AWS VPC Flow Logs</b>	Captures network conversation statistics with 5-minute aggregation
<b>Windows OS</b>	Security events at the OS level
<b>Linux OS</b>	Security events at the OS level
<b>Endpoint Security Solution</b>	Malicious code and unauthorized software events and Audit events for management console
<b>Database Security Tool</b>	Database events
<b>Database Server Logs</b>	Database events

Each application team is responsible for ensuring and Splunk for IRIS are ingesting audit event data from their system and creating queries as well as appropriate alerts for unusual or suspicious activity. The IRIS system constantly monitors for audit failures. This is implemented using Security Incident Event Management (SIEM) monitoring and Application and Service Monitoring. SIEM is configured to periodically inspect logs and alert IRIS Cloud Operations and Security team members when suspicious or unusual activity is detected.

## Incident response

Customers require an organized approach to managing the investigation and response to potential and confirmed incidents. CIP-008, Incident Reporting and Response Planning, defines requirements for planning, reporting and managing incident response, recovery and reconstitution. Infor practices incident response policies and programs that include incident response testing and is evaluated by independent, third-party assessors. Infor model leverages industrial best practices such as ITIL and the model is designed to comply with FedRAMP control implementation requirements, as well as other applicable laws, regulations, and standards. The sub-processes documented within the main process domains (Initiate, Qualify, Research and Resolve) serve as the underpinnings for the FedRAMP Incident Response family control implementation.

Should an incident or information spillage arise so severe that it compromises the business continuity operations of Infor personnel or customers, Infor will follow the appropriate Information System Contingency Plan for the affected applications and/or the Business Continuity Plan for support.

The Infor Incident Response lifecycle leverages an ITSM for the SaaS environment as the centralized monitoring and reporting tool. The information captured throughout the lifecycle of a confirmed incident response is in compliance with the United States Computer Emergency Readiness Team Reporting guidelines.

## Resilience and system recovery

Resilience and availability are paramount to grid reliability, Infor SaaS solutions architecture is designed with no single point of failure (application and hardware) ensuring the applications run consistently in one or more location as any given point. Our SaaS will be scaled accordingly to maintain optimal performance levels. Infor relies on AWS to leverage a sophisticated infrastructure, platform, and services that can scale virtually infinitely to ensure optimal performance.

Infor application and database servers are installed across multiple availability zones (AZ's) to provide the highest availability possible. If a data center or AZ partially or completely fails, the workload is automatically redistributed across the other AZ's within the region by the AWS Elastic Load Balancers (ELB) and Auto Scaling services. Relational database servers employ synchronous or near-synchronous replication to duplicate data in multiple AZ's to minimize or eliminate any transaction loss due to a system, data center, or AZ failure.

The backup schedule is weekly full, 8-hours differential and 15-minute transactional log with 14 days of retention. In the case of any disaster, automatic failover, no restore is required (however, the user/customer will need to login again to the system).

Documenting and testing recovery plans is critical to meeting the availability and resilience objectives for any organization. CIP-009, Recovery Plans for BES Cyber Systems, defines requirements for recovery planning, backup, and testing. Customers can use Infor SaaS offering for highly available and resilient applications.

## Physical security

CIP-006, Physical Security of BES Cyber Systems, requires each Responsible Entity to implement a documented physical security plan(s) that covers security measures such as physical access controls, and logging and monitoring of access (authorized and unauthorized). Infor customers inherit the AWS data center controls that physically secure the cloud infrastructure by strictly controlling access at the perimeter, at building ingress points, and to the data center floors. AWS allows physical data center access only to approved employees and authorized visitors. Access is logged and audited routinely. Physical access to data centers in AWS GovCloud (US) is restricted to people who have been validated as being US citizens.

## Planning considerations for use of cloud services

Each organization's cloud adoption journey is unique. To successfully migrate to the cloud, it is valuable to understand your organization's current state, the desired objectives, and the transition required to achieve those objectives. When setting goals, customers should take a risk-based approach to their implementation of their internal security requirements using Infor cloud solutions. This includes validating that your customer service agreement aligns with your internal security and resilience requirements; building detective controls, if needed, to ensure that processes are functioning as intended; and, updating processes to incorporate Infor solutions and services.

In the development process, collaboration with NERC or Regional Entities' auditors can be important to gaining confidence with compliance. Opening dialogue, being transparent, and understanding auditor perspectives and expectations can help you set goals and create work streams that not only enable staff to thrive in the cloud, but also help define evidence needs to support compliance demonstration.

Beyond this document, there are many other free resources available for customers to leverage during their cloud adoption journey, including whitepapers listed in the **Additional Resources** section of this paper and **computer-based trainings**. Customers seeking a closer partnership with Infor can also reach out to their Account Managers.

## Contributors

Contributors to this document include:

- Joe Arthur, VP Regulated Industries SaaS, Infor
- Mark Tomlinson, Cloud Solution Architect, Infor
- Claiborne Collier, Director Security and Compliance, Infor
- John Paddock, Compliance & Governance, Infor
- Jeremy Soehnlín, Sr. Cloud Solution Architect, Infor

## Additional Resources

For additional information, see:

- [NIST Cybersecurity Framework](#)
- [Infor Software as a Service \(SaaS\) Delivery Guide](#)
- [Federal Risk and Authorization Management Program \(FedRAMP\)](#)
- [AWS Power and Utilities page](#)
- [IDC Technology Spotlight–Cloud Adoption Unleashes Greater Value for Power and Utility Companies](#)
- [AWS FedRAMP page](#)
- [NIST Technical Note 2051–Cybersecurity Framework Smart Grid Profile](#)

# Appendix

## Infor solutions and services and alignment to NERC CIP

The following illustrates how Infor solutions and inherited controls can be used to demonstrate compliance with NERC CIP and provides an overview of customer considerations for security in the cloud. For CIP Standards and Requirements that are an Infor Responsibility, further details about the controls that have been implemented can be found in the assurance reports described previously. We have also mapped the CIP requirement to the NIST Cyber Security Framework (CSF).

---

### CIP-002 | Critical Cyber-Asset Identification

NERC Standards CIP-002 through CIP-009 each contribute to the cyber-security framework for the identification and protection of all Critical Cyber-Assets to support the reliable operation of the BES.

Each of these different standards recognizes the distinct roles of each entity within the operation of the BES. The standard also acknowledges the criticality and vulnerability of the assets involved that are necessary to manage BES for optimal reliability. Further, these standards serve to illuminate the risks to which the BES is regularly exposed.

CIP-002, in particular, requires the identification and documentation of any Critical Cyber-Assets associated with the determined Critical-Asset in question that supports the reliable operation of the BES through the performance of a **risk-based assessment by your auditing firm**.

---

### CIP-002-5.1a R1 | Critical Cyber-Asset Identification

#### CIP Requirement

“R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: [Violation Risk Factor: High][Time Horizon: Operations Planning]

- i. Control Centers and backup Control Centers;
- ii. Transmission stations and substations;
- iii. Generation resources;
- iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and
- vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems

according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

#### Customer Considerations

Customers can continue to follow their compliance program processes to meet BES Cyber System Categorization CIP standards to identify and categorize key cyber components and assets of their system in order ensure that they are appropriately protected according to regulatory requirements.

#### NIST CSF

**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent

## CIP-002-5.1a R1 | Critical Cyber-Asset Identification (continued)

---

with their relative importance to business objectives and the organization's risk strategy.

### Infor Responsibility

Infor solution provides three key benefits that can mitigate the challenges with maintaining asset inventories in an on-prem environment.

- **Infrastructure:** Infor has partnered with AWS for Infrastructure as a Service (IaaS) and AWS assumes sole responsibility for managing physical assets that comprise the AWS cloud infrastructure. This can significantly reduce the burden of physical asset management for customers for those workloads that are hosted in AWS. The customer would still be responsible for maintaining physical asset inventories for the equipment they keep in their environment (e.g., datacenters, offices, deployed IoT, mobile workforce, etc.).
- **Platform & Services:** Infor maintains deep visibility and asset inventory for logical assets hosted in a customer's SaaS account. It does not matter if an EC2 instance (virtual server) is turned on or off, whether the endpoint agent is installed and running, regardless of what network segment the asset is on, or any other factor. Infor can query and obtain visibility

of applications, platforms, and AWS infrastructure service assets. This reduces the inventory burden on Infor to the software installed on EC2 instances and what data assets are stored in AWS. Infor also uses other services that perform this capability, like Amazon Macie, which help identify, classify, label, and apply rules to data stored in Amazon S3.

- **Applications:** Infor provides secure Enterprise Asset Management and Supply Management solutions to help you solve your critical asset performance challenges to record, maintain, structure, and standardize asset information. It captures the identity, configuration, and structure of physical assets, their complete technical and commercial configurations, and current position (either by location, functional position, or tag) as well as past locations and maintenance history. Using IoT capabilities and reliability centered maintenance features of EAM, customers can track anomalies that require attention before they become critical. Infor Supply Management provides visibility and management execution activities in a single dashboard, thereby proactively eliminating bottlenecks and improving overall efficiency. End-to-end visibility enables you to make better decisions. More importantly, it enables rapid execution upon those decisions to improve system reliability.

## CIP-002-5.1a R2 | Critical Cyber-Asset Identification

---

### CIP Requirement

R2. The Responsible Entity shall:

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

### Customer Considerations

Customers can continue to follow their compliance program processes to meet BES Cyber System Categorization CIP standards to review and obtain approval of the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, in accordance with regulatory requirements.

### NIST CSF

**Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

### Infor Responsibility

Our BES offering is used in Infor Regulated Industries SaaS (IRIS) system run in AWS GovCloud region and follows FedRAMP security impact levels based on the potential impact definitions for each of the security objectives (i.e., confidentiality, integrity and availability) discussed in NIST SP 800-60 and FIPS Pub 199. The System Sensitivity Level has been designated at Moderate. Infor monitors at least annually and updates if there are any changes as approved by the Systems Owner.

## CIP-003 | Security Management Controls

---

CIP-003's purpose, within the framework of Standards CIP-002 through CIP-009, requires that all Responsible Entities have the minimum security management controls in place at all times to protect Critical Cyber-Assets.

With this standard, the Responsible Entity must document and implement a sound cyber-security policy that accurately represents management's ability and commitment to security all Critical Cyber-Assets under his or her care. Such responsibilities in this standard certainly include all provisions regarding emergency situations.

Additionally, the Responsible Entity must ensure that the completed cyber-security policy is readily available to all personnel who are responsible for, or who have access to, any Critical Cyber-Assets.

Finally, the cyber-security policy must undergo review each year by the senior manager assigned to the task.

## CIP-003-7 R1 | Security Management Controls

---

### CIP Requirement

Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics:

- 1.1 For its high impact and medium impact BES Cyber Systems, if any:
  - 1.1.1. Personnel and training (CIP-004);
  - 1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
  - 1.1.3. Physical security of BES Cyber Systems (CIP-006);
  - 1.1.4. System security management (CIP-007);
  - 1.1.5. Incident reporting and response planning (CIP-008);
  - 1.1.6. Recovery plans for BES Cyber Systems (CIP-009);
  - 1.1.7. Configuration change management and vulnerability assessments (CIP-010);
  - 1.1.8. Information protection (CIP-011); and
  - 1.1.9. Declaring and responding to CIP Exceptional Circumstances.
- 1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:
  - 1.2.1. Cyber security awareness;
  - 1.2.2. Physical security controls;
  - 1.2.3. Electronic access controls for Low Impact External Routable Connectivity (LERC) and Dial-up Connectivity; and
  - 1.2.4. Cyber Security Incident response
  - 1.2.5. Transient Cyber Assets and Removable Media malicious code risk mitigation; and
  - 1.2.6. Declaring and responding to CIP Exceptional Circumstances.

### Customer Considerations

Customers can continue to follow their compliance program processes to meet BES Cyber System review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address high impact and medium systems in order ensure that they are appropriately protected according to regulatory requirements.

### NIST CSF

**Governance (ID.GV):** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

### Infor Responsibility

Infor's journey to FedRAMP Authorization has necessarily meant profound, if gradual, shifts in the way information technology (IT) meets the needs of business users. As its own cloud offerings have begun to mature, Infor recognizes that new approaches to IT governance are necessary to realize the full power of the cloud required to effect business transformation. IRIS Governance, a broad organizational and philosophical structure, has evolved to recognize the challenges and opportunities posed by the cloud and to ensure a smooth transition using Infor's "3C Approach" – Cloud, Convergence and Compliance.



## CIP-003-7 R1 | Security Management Controls (continued)

---

Convergence means standardizing on the FedRAMP security framework for technologies, platforms, and processes, and using it as an overlay for other security compliance standards. Compliance focuses on adhering to a risk-based management approach, prescribed to improve real-time security visibility between cloud service providers and their Government customers. Infor remains committed to the regulatory compliance of the FedRAMP security assessment, authorization and continuous monitoring investments aimed at improving the information assurance of Infor application and solutions offered by and through IRIS. Consolidation seeks to

eliminate redundancies and actively drive convergence at every opportunity, be it on simplified compliance documentation and reporting to streamlined on-boarding applications or technology refresh. Cloud directive provides the framework to move all IT services to the Cloud, Application development using Cloud Foundry and Desktop or mobile virtualization. Cloud migration is an integral part of Infor's architectural strategy, and FedRAMP compliance will provide the entry for Infor to conduct business within the regulated industries Software as a Service (SaaS) market.

## CIP-003-7 R2 | Security Management Controls

---

### CIP Requirement

Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

### Customer Considerations

Customers can continue to follow their compliance program processes to implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that ensure that they are appropriately protected according to regulatory requirements.

### NIST CSF

**Asset Management (ID.AM-1):** Physical devices and systems within the organization are inventoried

### Infor Responsibility

Infor tracks and maintains 100% of the devices and systems we manage, and we partnered with AWS for infrastructure and related services and they manage and maintain 100% for the physical devices and systems within their data centers.

## CIP-003-7 R3 | Security Management Controls

---

### CIP Requirement

Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.

### Customer Considerations

Customers can continue to follow their compliance program processes for CIP Senior Manager identification by name and document any changes within 30 days according to regulatory requirements.

### NIST CSF

**Governance (ID.GV-1):** Organizational information security policy is established

### Infor Responsibility

Infor Governance charter includes organizational security policy that identifies key individuals, including the System Owner. Infor practice is to document leadership changes within 30 calendar days of the change.

## CIP-003-7 R4 | Security Management Controls

---

### CIP Requirement

The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.

### Customer Considerations

Customers can continue to follow their compliance program processes for CIP Senior Manager delegation of authority that is updated within 30 days according to regulatory requirements.

## CIP-004 | Personnel & Training

---

Standard CIP-004 requires that each member of the team who has access to any Critical Cyber-Assets—whether authorized cyber access or authorized unescorted access to physical assets—have the appropriate amount and level of personnel risk assessment credentials, training and security awareness. Persons in this category may include contractors and service vendors.

Following are more details on the necessary requirements in awareness and training for employees.

### Awareness

Each Responsible Entity must establish, maintain and document a security awareness program to make sure all personnel are continually compliant with this standard. A few of the key components of such a program include instruction regarding appropriate behavior for the following situations:

## CIP-004 | Personnel & Training

---

### CIP Requirement

Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-6 Table R1 – Security Awareness Program. (please see standard for sub-req's)

### NIST CSF

**Governance (ID.GV-1):** Organizational information security policy is established

### Infor Responsibility

Infor Governance charter includes organizational security policy, including roles and responsibilities, that is further defined in our System Security Plan, Security Incident Response Plan, and other related plans and guidance. Delegation authority is documented in the applicable plans.

- Direct communications that may include emails, memos and computer-based training
- Indirect communications that may indicate posters, intranet, brochures and newsletters
- Management support and reinforcement in settings like presentations and meetings

### Training

Training will serve to reinforce the components of awareness. Each relevant personnel member must undergo proper awareness training within ninety calendar days of authorization to physical assets or Critical Cyber-Assets.

### Customer Considerations

Customers can continue to follow their compliance program processes to documented security awareness program for each applicable security requirement.

## CIP-004-6 R1 | Personnel & Training (continued)

---

### NIST CSF

**Governance (ID.GV-2):** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners

### Infor Responsibility

Infor Global Policies directs the activities within the Infor Training Process. The procedure document addresses purpose, scope, responsibilities (including management commitment), coordination among organizational entities, and compliance

requirements to meet the applicable control implementation requirements for the awareness and training. This training maps back to applicable CIP-004-6 Table R1 requirements. The plan specifically addresses procedures or processes related to:

- Course registration and training intervals
- Course completion for IRIS security training (security awareness and role-based)
- Training records
- Manager reports

## CIP-004-6 R2 | Personnel & Training

---

### CIP Requirement

Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-6 Table R2 – Cyber Security Training Program. (please see standard for sub-req's)

### Customer Considerations

Customers can continue to follow their compliance program processes to provide cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts.

### NIST CSF

**Awareness and Training (PR.AT):** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements

### Infor Responsibility

Infor Cyber Security Training Program is tailored to ensure compliance alignment, including CIP-004-6 R2 requirements. Infor provides cybersecurity training with an emphasis on individual roles, functions, and responsibilities via Infor Learning Management System (LMS). Training completion based on their specific roles is verified before granting access and part of the annual cybersecurity training program.

## CIP-004-6 R3 | Personnel & Training

---

### CIP Requirement

Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in CIP-004-6 Table R3 – Personnel Risk Assessment Program. (please see standard for sub-req's)

### Customer Considerations

Customers can continue to follow their compliance program processes to documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that meet systems security management controls requirements.

### NIST CSF

**Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

## CIP-004-6 R3 | Personnel & Training

---

### Infor Responsibility

All Infor personnel are screened prior to gaining access to Infor Cloud SaaS infrastructure. Infor employs a third-party vendor to perform background investigations on all employees before hiring. This includes a seven-year criminal history records check as part of the personnel risk assessment during the hiring process and periodically to national security clearance

requirements based on security impact and/or clearance levels. Verification that all applicable security screening has been completed, including criminal history records check, is performed before authorizing access for personnel, contractors, and service vendors to IRIS.

## CIP-004-6 R4 | Personnel & Training

---

### CIP Requirement

Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. (please see standard for sub-req's)

### Customer Considerations

Customers can continue to follow their compliance program processes to documented access management program(s) that collectively include each of the applicable requirement that meet systems security management controls requirements.

### NIST CSF

**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

### Infor Responsibility

Infor “Security Policy” directs the activities within IRIS Identity and Access Management (IAM) procedure. The plan addresses purpose, scope, responsibilities (including management commitment), coordination among organizational entities, and compliance requirements to meet the FedRAMP and NIST control implementation requirements for the access control

family of a moderate baseline. The Access Management Plan aligns with CIP-004-6 Table R4 and addresses topics related to:

- Information Access Restriction (e.g., least privilege and separation of duties)
- The Request Fulfillment Process for Provisioning GovCloud Access
- Managing the Administrative privileges
- The Periodic Review of GovCloud Access
- The Revocation of GovCloud Access
- The Separation of Duties
- Password Policy
- Access Control to Program Source Code
- Authenticator Device Management
- Physical access to assets is managed and protected (AWS)
- Network integrity is protected (e.g., network segregation, network segmentation)
- Infor policies and procedures are captured in Infor’s document repository management system and reviewed within FedRAMP / NIST requirements by the document owner.

## CIP-004-6 R5 | Personnel & Training

---

### CIP Requirement

Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R5 – Access Revocation. (please see standard for sub-req's)

### Customer Considerations

Customers can continue to follow their compliance program processes to documented access revocation program(s) that collectively include each of the applicable CIP controls requirements.

### NIST CSF

#### Information Protection Processes and Procedures

**(PR.IP-11):** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)

#### Infor Responsibility

Infor IAM procedure (see response to CIP-004-6 R4) includes the revocation of access within 24 hours of termination, reassignment, or transfers

## CIP-005 | Electronic Security Perimeter(s)

---

Standard CIP-005 requires the protection and identification of the Electronic Security Perimeter(s). Such an area houses all Critical Cyber-Assets and all access points along the perimeter.

The assigned Responsible Entity is required to maintain the security of the area surrounding all Cyber-Security Assets, using the following criteria, in addition to the Electronic Security Perimeter(s) itself:

- Electronic Access Controls
- Monitoring Electronic Access
- Cyber-Vulnerability Assessment
- Documentation Review and Maintenance

## CIP-005-6 R1 | Electronic Security Perimeter(s)

---

### CIP Requirement

Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-6 Table R1 – Electronic Security Perimeter*.

### Customer Considerations

Customers can continue to follow their compliance program to implement the documented processes for electronic security perimeter that collectively include each of the applicable CIP controls requirements.

### NIST CSF

**Access Control (PR.AC-5):** Network integrity is protected, incorporating network segregation where appropriate

#### Infor Responsibility

Infor deploys IRIS applications in AWS GovCloud so all system admin access is considered remote. IRIS Global Policies articulate the following for remote access:

- The IRIS Access Management Plan documents and provides procedures for enforcement, usage restrictions, and implementation guidance for each allowed remote access method.
- DUO Time-based One-time Passwords (TOTP) meet the requirements for E-Authentication Level 3;

## CIP-005-6 R1 | Electronic Security Perimeter(s) (continued)

---

- IRIS monitors for unauthorized remote access and takes appropriate actions to terminate the session if unauthorized access is discovered.
- Remote access shall employ cryptography to protect session confidentiality and integrity such as using Transport Layer Security (TLS) 1.2.
- Remote access shall be routed through a designated port, only.
- Privileged commands and access to security-relevant information via remote access shall only be permitted as described in the System Security Plan (SSP).

## CIP-005-6 R2 | Electronic Security Perimeter(s)

---

### CIP Requirement

Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-6 Table R2 – Interactive Remote Access Management*.

### Customer Considerations

Customers can continue to follow their compliance program to implement the documented processes for interactive remote access management that collectively include each of the applicable CIP controls requirements.

### NIST CSF

**Access Control (PR.AC-3):** Remote access is managed

### Infor Responsibility

Infrastructure administrative remote access to the IRIS environment is only available through the Remote Desktop Gateway Hosts (RDGW). All infrastructure remote access is provided through Remote Desktop Protocol (RDP) connections to the Remote Desktop Gateway Hosts. After authenticating with user ID, password and Duo Multifactor Time-based One-time password, administrators may further connect to their target server utilizing RDP or SSH. All SSH traffic will pass through the encrypted RDP connection provided by the RDGW.

## CIP-006 | Physical Security of BES Cyber Systems

---

Standard CIP-006 intends to secure the implementation of a physical security program to protect Critical Cyber-Assets.

The Physical Security Plan should address matters that include the following:

- Designating, identifying and documenting the Electronic Security Perimeter(s)
- Identifying all access points through each Physical Security Perimeter and measures to control entry via those access points
- Developing processes, tools and procedures necessary to monitor physical access to all relevant perimeters
- Designing a loss or breach response to manage any infiltrations to these areas

The Physical Security Plan must undergo review annually.

## CIP-006-6 R1 | Physical Security of BES Cyber Systems

---

### CIP Requirement

Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan*. (please see standard for sub-req's)

### Customer Considerations

Customers can continue to follow their compliance program to implement the documented processes for physical security plan(s) that collectively include each of the applicable CIP controls requirements.

### NIST CSF

**Access Control (PR.AC-2):** Physical access to assets is managed and protected

### Infor Responsibility

Infor has partnered with AWS for Infrastructure as a Service (IaaS). AWS data centers are state of the art, utilizing innovative

architectural and engineering approaches. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in facilities that are not branded as AWS facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.

Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

## CIP-006-6 R2 | Physical Security of BES Cyber Systems

---

### CIP Requirement

Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program*. (please see standard for sub-req's)

### Customer Considerations

Customers can continue to follow their compliance program to implement the documented processes for visitor control program(s) that collectively include each of the applicable CIP controls requirements.

### NIST CSF

**Access Control (PR.AC-2):** Physical access to assets is managed and protected

### Infor Responsibility

Infor has partnered with AWS for Infrastructure as a Service (IaaS). AWS maintains a Visitor Control Program that require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter. This includes manual or automated logging of visitors into and exit from the Physical Security Perimeter as required by CIP-006 Table R2.

## CIP-006-6 R3 | Physical Security of BES Cyber Systems

---

### CIP Requirement

Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-6 Table R3 – Maintenance and Testing Program*. (please see standard for sub-req's)

### Customer Considerations

Customers can continue to follow their compliance program to implement the documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable CIP controls requirements.

## CIP-007 | System Security Management

---

Standard CIP-007 focuses on the requirement of Responsible Entities to define methods, processes and procedures to secure all systems designated as Critical Cyber-Assets, along with non-critical Cyber-Assets that lie within the Electronic Security Perimeter(s).

Following are the methods, processes, practices, policies and tools needed to comply with the CIP-007 Standard:

- Test Procedures
- Ports and Services
- Security Patch Management
- Malicious Software Prevention
- Account Management
- Security Status Monitoring
- Disposal or Redeployment
- Cyber-Vulnerability Assessment
- Documentation Review and Maintenance

## CIP-007-6 R1 | System Security Management

---

### CIP Requirement

Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R1 – Ports and Services*. (please see standard for sub-req's)

Customers maintain ownership and control over their content in the cloud and are responsible for managing who can access their tenants and role-based security policies and user setup.

### NIST CSF

**Access Control (PR.AC-2):** Physical access to assets is managed and protected

**Maintenance (PR.MA-2):** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

### Infor Responsibility

Infor has partnered with AWS for Infrastructure as a Service (IaaS). AWS provides maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.



## CIP-007-6 R1 | System Security Management (continued)

---

### NIST CSF

**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions

### Infor Responsibility

Infor is responsible for the systems in the cloud and for managing security requirements, including restricting ports and services, patch management, malicious code prevention, security event monitoring, and system access control. Infor uses VPC(s) to manage ports and services access and to restrict traffic to specific ports and source/ destination CIDRs by using

security groups and network ACLs. Amazon S3 Access Points are used to limit access to S3 data and data lakes to specific VPCs. Different sets of permission are granted to fine tune access. With Amazon S3 Access Points S3 data never leaves the customer's VPC. (CIP-007-6, R1)

AWS is responsible for the security of the physical cloud infrastructure and has demonstrated compliance with multiple control frameworks, addressing controls for systems and network security for the cloud infrastructure.

Infor customers inherit these controls and can reference our assurance reports demonstrating the validity of our controls. (CIP007-6, R1-R5)

## CIP-007-6 R2 | System Security Management

---

### CIP Requirement

Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R2 – Security Patch Management*. (please see standard for sub-req's)

### Customer Considerations

Customers can continue to follow their compliance program processes to meet systems security management controls requirements. Customer should be aware of Infor security patch management approach and processes and incorporate into their compliance program.

### NIST CSF

**Maintenance (PR.MA-1):** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools

### Infor Responsibility

Infor, like many SaaS-focused organizations, is moving to a versionless software solution. New functionality and updates, including security patches, are released monthly, as needed. Infor manages upgrading unmodified environments to the current version of the Subscription Software. Infor follows ITIL and NIST standards for change management and will provide notifications and release notes for any changes to the applications, per the terms of our SLA.

Infor Security Monitoring and Vulnerability Management Plan specifically addresses procedures or processes related to:

- Vulnerability Management & Continuous Monitoring
- Critical Milestones and Service Level Agreements
- Vulnerability Remediation
- Vulnerability Scanning Tool Work Instructions
- Security Monitoring

Infor conducts assessments 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 based on the Infor Risk Management Framework, which was constructed in accordance the National Institute of Standards and

Technology (NIST) SP 800-39 and the risk assessment process as detailed in NIST SP 800-30. These assessments ensure all policies and supporting procedures properly address the boundary authorization in accordance with changing regulatory, contractual, business, technical, and operational requirements.

Infor has implemented a continuous monitoring strategy to support its FedRAMP and other regulatory compliance requirements. The strategy requires that Infor risk assessments take place annually, or more frequently as circumstances necessitate. The risk assessments illustrate the effectiveness of existing information security controls and safeguards, as well as the identity of new risks.

### CIP Requirement

Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R3 – Malicious Code Prevention*. (please see standard for sub-req's)

### Customer Considerations

Customers can continue to follow their compliance program processes to meet systems security management controls requirements for any code development they perform and maintain and ensure documented processes are implemented for malicious code prevention.

### NIST CSF

#### Information Protection Processes and Procedures (PR.

**IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets

**Data Security (PR.DS-6):** Integrity checking mechanisms are used to verify software, firmware, and information integrity

### Infor Responsibility

Infor implements non-signature based malicious code detection such as heuristics or anomalous behavior detection. This is used to detect malicious code without any prior knowledge of the malicious code. Infor's non-signature-based detection makes determination based on a file's characteristics and behavior.

Some of the techniques to be included in a multi-layered security approach include the following:

- **Variant Protection**—Variant protection looks for obfuscated, polymorphic or variants of malware by using fragment of previously seen malware and detection algorithms.
- **Census**—The likelihood that a file is malicious can be determined in part by its prevalence and maturity (i.e., how often it has been seen over a given time period). Files that have never been detected are considered to be more suspicious. This technique has proven to be quite strong against malware hash factories.
- **(Planned implementation) Whitelisting**—To reduce false positives on endpoint detections, all files should be checked against a database of known and verified safe files. (Trend Micro's certified safe software whitelist contains almost one billion known safe files.)
- **Behavioral Analysis**—This technique examines an item as it is unpacked, looking for suspicious or unusual behavior in how it interacts with operating systems, applications and scripts—even if the item isn't on a blacklist. While crypto-ransomware can easily pass by traditional anti-virus (by being a freshly compiled executable), it will behave suspiciously as it loads into memory, triggering further action. As attackers are still finding it difficult to evade behavior-based detection, this technique is a must-have for any organization.

When malicious code is identified, alerts are sent to the defined security personnel in the incident response plan, for investigation. Appropriate actions are promptly taken to correct the problem.

## CIP-007-6 R4 | System Security Management

---

### CIP Requirement

Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R4 – Security Event Monitoring*. (please see standard for sub-req's)

### Customer Considerations

Customers can continue to follow their compliance program processes to meet systems security management controls requirements for any systems they manage and ensure documented processes are implemented for Security Event Monitoring.

### NIST CSF

#### Information Protection Processes and Procedures

**(PR.IP-12):** A vulnerability management plan is developed and implemented

### Infor Responsibility

Infor's Vulnerability Management Plan (VMP) addresses how security vulnerabilities are identified and documented, how threats, vulnerabilities, likelihoods, and impacts are used to determine risk, and how risk responses are identified and prioritized. Infor's Security Incident Response Plan (SIRP) explains

how cyber threat intelligence is received from information sharing forums and sources, along with threats, both internal and external, are identified and documented, and how potential business impacts and likelihoods are identified. Infor solution meets CIP-007-6 Table R4 requirements.

The VMP and SIRP plans documents the processes to adequately prepare, detect, analyze, contain, eradicate and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to software, systems configuration, or data (e.g., malicious logic, such as a virus, worm, or Trojan horse). It also provides Infor personnel and partners with a roadmap for managing its security incident response capability in a structured and consistent manner necessary to mitigate incidents posing a threat or operational risk exposure to the environment.

Infor incorporated The Federal Risk and Authorization Management Program (FedRAMP) requirements based on the NIST SP 800-61, Computer Security Incident Handling Guide, to meet the unique requirements of a Low, Moderate or High Control Baseline implementations. All Federal entities are required to ensure the cloud systems they use for hosting government data comply with the FedRAMP requirements. More information on FedRAMP can be found here: <https://www.fedramp.gov/>

## CIP-007-6 R5 | System Security Management

---

### CIP Requirement

Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R5 – System Access Controls*. (please see standard for sub-req's)

### Customer Considerations

Customers can continue to follow their compliance program processes to meet system access control requirements. Customers can use their existing directory service provided it is SCIM 2.0 and supports SAML 2 to support interactive user authentication and account management. (CIP007-6, R5)

### NIST CSF

**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

### Infor Responsibility

In the cloud, these requirements can be addressed by managing access to perform cloud configuration and management activities; remote access to servers in the cloud; and end user access to applications. Infor uses several tools and services to manage users that meet or exceed CIP-007-6 Table R5 requirements that includes:

**Customer IAM:** Customer provided identity management solutions will be used by IRIS to allow customer user access via SAML assertions. Groups, roles, and access authorization rights

## CIP-007-6 R4 | System Security Management (continued)

---

in IRIS applications are configurable by the customer. It is a customer responsibility to create or customize IRIS application groups, roles, and access authorization rights appropriate for their organization, approve access authorizations including group membership and assign users to IRIS application groups.

**Infor Privileged User IAM:** The personnel roles and privileges documented Infor's FedRAMP System Security Plan (SSP) correspond to the mission/business functions of the CloudOps and SecOps teams that support the IRIS environment:

- **CloudOps Team**—Comprised of network, database, and system administrators that manage the overall operation of IRIS infrastructure and applications with system roles, details provided in SSP.
- **SecOps Team**—Comprised of Security Analysts with system roles, details provided in SSP.

## CIP-008 | Incident Reporting and Response Planning

---

Standard CIP-008 prepares entities for any incidents that arise, ensuring the identification, classification, response, and reporting and documentation of Cyber-Security Incidents related to Critical Cyber-Security Assets.

With this standard, the Responsible Entity must develop and maintain a Cyber-Security Incident Response Plan. He or she

must also implement the resulting plan that includes proper reporting procedures to all relevant authorities.

Additionally, the Responsible Entity must keep all relevant documentation related to any incidents.

## CIP-008-5 R1 | Incident Reporting and Response Planning

---

### CIP Requirement

Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*.

### Customer Considerations

Customers can continue to follow their compliance program processes to meet incident reporting and response planning requirements. Response plans should be reviewed and updated to incorporate use of Infor Solutions that support incident detection and response. (CIP008-5, R1-R3)

### NIST CSF

#### **Information Protection Processes and Procedures (PR.IP-9):**

Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed

### Infor Responsibility

Infor's Security Incident Response Plan (SIRP) mitigates the risk to the reliable operation of IRIS solutions that can support CIP-008-5 Table R1. Infor SIRP in combination with our EAM solution can be configured to provide feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Infor SIRP includes preventative activities that work to lower the number of incidents and preplanned incident response capability for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. Infor' enterprise incident response system used for all IRIS customers is used to meet the requirements.

## CIP-008-5 R2 | Incident Reporting and Response Planning

---

### CIP Requirement

Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.

### Customer Considerations

Customers can continue to follow their compliance program processes to meet incident reporting and response planning requirements. Response plans should be reviewed and updated to incorporate use of Infor Solutions that support incident detection and response. (CIP008-5, R1-R3)

### NIST CSF

#### Information Protection Processes and Procedures

**(PR.IP-10):** Response and recovery plans are tested

### Infor Responsibility

Infor follows the SIRP when responding to a reportable cyber security incident or performing an exercise of a reportable cyber security incident and document deviations from the plan(s) taken during the response to the incident or exercise. Infor test the SIRP annually and retain records related to reportable cyber security incidents in alignment with CIP-008-5 Table R2.

To ensure the effectiveness of the SIRP, Infor conducts incident response testing. This testing provides excellent coverage for the discovery of previously unknown defects and failure modes. In addition, it allows the Infor Security and Service teams to test the systems for potential customer impact and further prepare staff to handle incidents such as detection and analysis, containment, eradication, and recovery, and post-incident activities.

## CIP-008-5 R3 | Incident Reporting and Response Planning

---

### CIP Requirement

Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*.

### Customer Considerations

Customers can continue to follow their compliance program processes to meet incident reporting and response planning requirements. Response plans should be reviewed and updated to incorporate use of Infor Solutions that support incident response plan review, update, and communication. (CIP008-5, R1-R3)

### NIST CSF

#### Information Protection Processes and Procedures (PR.IP-9):

Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed

### Infor Responsibility

Infor conduct's ongoing reviews, updates and communications to verify the SIRP response plan's effectiveness and consistent application in responding to a cyber security incident(s) impacting customers. Infor SIRP is designed to support High or Medium Impact BES Cyber Systems as outlined in CIP-008-5 Table R3.

The Incident Response Test Plan is executed annually, in conjunction with the SIRP. Infor incident management planning, testing and test results are reviewed by third party auditors.

## CIP-009 | Recovery Plans for BES Cyber Systems

---

This standard ensures that recovery plan(s) are developed for Critical Cyber-Assets. Standard CIP-009 also provides that these plans follow established business continuity and any disaster recovery plans, techniques or practices.

The Responsible Entity must create and review recovery plan(s) annually for any Critical Cyber-Assets in his or her care.

At the very minimum, the recovery plan(s) must address required actions to respond to an event or condition of varying duration and severity that might necessitate the activation of the required recovery plan(s). It is also essential to define the roles and responsibilities of each responder on the team.

The following components must also be included in recovery plan(s) to ensure effectiveness of the official Recovery Plans for Critical Cyber-Assets:

- Exercises. It is important to exercise the recovery plan(s) annually, at least, to test soundness and effectiveness for current conditions.
- Change Control. Upon learning the results of exercises, recovery plan(s) are subject to updates to reflect changes, or the need to make changes.
- Backup and Restore. Processes and procedures related to backup and storage of information needed to securely store Critical Cyber-Assets must regularly be performed.
- Testing Backup Media. Any information vital to recovery must be stored on backup media that undergoes annual testing, which may occur offsite.

## CIP-009-6 R1 | Recovery Plans for BES Cyber Systems

---

### CIP Requirement

Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in *CIP-009-6 Table R1 – Recovery Plan Specifications*. (please see standard for sub-req's)

### Customer Considerations

Customers can continue to follow their compliance program processes to meet recovery planning, backup and testing requirements. Customers are responsible for properly implementing contingency planning, training, and testing for their own systems. Recovery plans should be reviewed and updated to incorporate use of Infor solutions that support backup and recovery processes. (CIP-009-6 R1-R3)

### NIST CSF

#### Information Protection Processes and Procedures (PR.IP-9):

Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed

### Infor Responsibility

Infor Information System Contingency Plan (ISCP) addresses purpose, scope, responsibilities (including management commitment), coordination among organizational entities, and compliance requirements to meet the FedRAMP control implementation requirements for the contingency planning. The plan specifically addresses procedures or processes related to:

- Data Back-up
- Activation Criteria
- Notification and Communication
- Outage Assessment
- Recovery and Reconstitution
- Clean-Up

The ISCP is a preplanned recovery capability that is necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore system functionality occurs. (CIP-009-6, R1-R3)

## CIP-009-6 R2 | Recovery Plans for BES Cyber Systems

---

### CIP Requirement

Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-6 Table R2 – Recovery Plan Implementation and Testing*. (please see standard for sub-req's)

### Customer Considerations

Customers can continue to follow their compliance program processes to meet recovery planning, backup and testing requirements. Customers are responsible for properly implementing contingency planning, training, and testing for their own systems. Recovery plans should be reviewed and updated to incorporate use of Infor solutions that support backup and recovery processes. (CIP-009-6 R1-R3)

### NIST CSF

#### Information Protection Processes and Procedures (PR.IP-4):

Backups of information are conducted, maintained, and tested periodically

**(PR.IP-10):** Response and recovery plans are tested

### Infor Responsibility

Infor ISCP has been developed to recover and reconstitute the IRIS system using a three-phased approach. The approach ensures that system recovery and reconstitution efforts are performed in a methodical sequence to maximize the effectiveness of the recovery and reconstitution efforts and minimize system outage time due to errors and omissions. The three system recovery phases consist of activation and notification, recovery, and reconstitution.

Infor ISCP serves to mitigate the risk to the reliable operations by reducing the time to recover from various hazards affecting IRIS Systems and ensures continued implementation of the response plans. Infor's backup approach and use of multiple AWS availability zones provides further assurance recover systems and data.

Infor design leverages AWS ubiquitous security control environment across all regions. Each data center is built to physical, environmental, and security standards in an active-active configuration, employing redundancy to ensure system availability in the event of component failure. (CIP-009-6, R1-R3)

## CIP-009-6 R3 | Recovery Plans for BES Cyber Systems

---

### CIP Requirement

Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication*. (please see standard for sub-req's)

### Customer Considerations

Customers can follow their compliance program processes to meet recovery planning requirements for documenting lessons learned, update recovery plans, and notify identified persons or groups of the updates. Plans should be reviewed and updated to incorporate use of Infor Solutions that support *Recovery Plan Review, Update and Communication*. (CIP-009-6 R1-R3)

### NIST CSF

#### Information Protection Processes and Procedures (PR.IP-9):

Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed

### Infor Responsibility

Infor ISCP recovery and reconstitution process improves the effectiveness of recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Infor approach achieves the following action:

- Performing a “lessons-learned” review
- Revising the plan based on specific changes in the organization or technology that would impact plan execution.

In both instances when the plan needs to change, the Infor updates and distributes the plan. (CIP-009-6 R3)

## CIP-010 | Configuration Change Management and Vulnerability Assessments

---

This standard purpose is the prevention and detection of unauthorized changes to Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

The following areas should be addressed as part of the configuration change management and vulnerability assessments:

- Develop and maintain baseline configurations
- Record and document any change that deviate from the baseline configuration
- Update the baseline. configuration after a change
- Test or verify security the controls impacted by a change
- Monitor the baseline configuration at least every 35 days
- Conduct vulnerability assessments.

### CIP-010-3 R1 | Configuration Change Management and Vulnerability Assessments

---

#### CIP Requirement

Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management*. (please see standard for sub-req's)

#### Customer Considerations

Customers can continue to follow their compliance program processes to meet configuration change management and vulnerability assessment requirements. Plans should be reviewed and updated to incorporate use of Infor Solutions that support configuration change management. (CIP-010-3 R1-R4)

#### NIST CSF

##### Information Protection Processes and Procedures (PR.IP-1):

A baseline configuration of information technology/industrial control systems is created and maintained

**(PR.IP-3):** Configuration change control processes are in place

#### Infor Responsibility

Infor has chosen to adopt the Configuration Management principles established in NIST SP 800-53 “Configuration Management,” Control Family guidelines, as the official

policy for this domain. The following subsections outline the Configuration Management standards that constitute Infor policy. The IRIS is bound by this policy.

- CM-1 Configuration Management Policy and Procedures
- CM-2 Baseline Configuration
- CM-3 Configuration Change Control
- CM-4 Security Impact Analysis
- CM-5 Access Restrictions for Change
- CM-6 Configuration Settings:
- CM-7 Least Functionality
- CM-8 Information System Component Inventory
- CM-9 Configuration Management Plan
- CM-10 Software Usage Restrictions

Infor applies a systematic approach to managing change to ensure that all changes are reviewed, tested, and approved. (CIP-010-2, R1- R2)



## CIP-010-3 R2 | Configuration Change Management and Vulnerability Assessments

---

### CIP Requirement

Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R2 – Configuration Monitoring*. (please see standard for sub-req's)

### Customer Considerations

Customers can continue to follow their compliance program processes to meet configuration monitoring requirements. Plans should be reviewed and updated to incorporate use of Infor Solutions that support configuration monitoring. (CIP-010-3 R1-R4)

### NIST CSF

#### Information Protection Processes and Procedures (PR.IP-1):

A baseline configuration of information technology/industrial control systems is created and maintained

**(PR.IP-3):** Configuration change control processes are in place

#### Infor Responsibility

Infor Configuration Management plan addresses our configuration monitoring processes to detect unauthorized modifications IRIS Systems. Configuration monitoring is ongoing and performed, at least, monthly for changes. Any unauthorized changes detected are documented and investigated. (CIP-010-3 R2)

## CIP-010-3 R3 | Configuration Change Management and Vulnerability Assessments

---

### CIP Requirement

Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. (please see standard for sub-req's)

### Customer Considerations

Customers can continue to follow their compliance program processes to meet vulnerability assessments requirements. Plans should be reviewed and updated to incorporate use of Infor Solutions that support vulnerability assessments. (CIP-010-3 R1-R4)

### NIST CSF

#### Information Protection Processes and Procedures

**(PR.IP-12):** A vulnerability management plan is developed and implemented

#### Infor Responsibility

Infor's Vulnerability Management Plan (VMP) addresses how security vulnerabilities are identified and documented, how threats, vulnerabilities, likelihoods, and impacts are used to determine risk, and how risk responses are identified and prioritized. Infor's Security Incident Response Plan (SIRP) explains how cyber threat intelligence is received from information sharing forums and sources, along with threats, both internal and external, are identified and documented, and how potential business impacts and likelihoods are identified. Infor solution meets CIP-010-3 Table R3 requirements.

Infor Security notifies and coordinates with the appropriate service teams when conducting security-related activities within the system boundary. Activities include vulnerability scanning, contingency testing, and incident response exercises. Infor performs external vulnerability assessments at least annually, and identified issues are investigated and tracked to resolution. Additionally, Infor performs unannounced penetration tests by engaging independent third parties to probe the defenses and device configuration settings within the system.

## CIP-010-3 R4 | Configuration Change Management and Vulnerability Assessments

---

### CIP Requirement

Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1.

### Customer Considerations

Customers can continue to follow their compliance program processes to meet information protection requirements for Transient Cyber Assets and Removable Media. (CIP-010-3 R1-R4)

### NIST CSF

**Access Control (PR.AC-1):** Identities and credentials are managed for authorized devices and users

**Protective Technology (PR.PT-2):** Removable media is protected and its use restricted according to policy.

## CIP 011 | Information Protection

---

This standard purpose is to prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

### Infor Responsibility

Infor Regulated Industries SaaS (IRIS) is a cloud solution and do not allow external connections or 3rd party integrations without going through a security assessment process. Since we are a cloud solution we do not allow for any removable media access to our environment.

IRIS does provide authorized ingress and egress paths that allows approved integrations/data transfers. Infor works closely with our customers to assess all IRIS integrations and formally review in advanced to insure they meet minimum security requirements and are cloud friendly.

This approach helps to customers meet the following security objectives (CIP-010-3 R4):

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

The following areas should be addressed as part of the information protection activities:

- Document process to identify BES Cyber System Information
- Develop and maintain evidence of processes or procedures that address Information Protections

## CIP-011-2 R1 | Information Protection

---

### CIP Requirement

Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection*. (please see standard for sub-req's)

### Customer Considerations

Customers can continue to follow their compliance program processes to meet information protection requirements. (CIP-011-2 R1-R2)

### NIST CSF

**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

### Infor Responsibility

Infor ensures the confidentiality and integrity of transmitted information by employing cryptographic protection. All access to the applications is through the NGINX reverse proxies which enforce HTTPS via TLS sessions only. Communication to the AWS Management Console and AWS APIs also utilize TLS encryption that is provided and controlled by AWS as part of its FedRAMP offering.

Infrastructure administrative access to the IRIS environment is through the Remote Desktop Gateway (RDGW) hosts with confidentiality and integrity provided by RDP over TLS. After authenticating to the Remote Desktop Gateway host using user ID, password and DUO multifactor authentication, Administrators may further connect to their target server utilizing RDP or SSH. All SSH traffic will pass through the encrypted RDP over TLS connection between the administrators' computer and the RDGW host.

## CIP-011-2 R2 | Information Protection

---

### CIP Requirement

Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal*. (please see standard for sub-req's)

### Customer Considerations

Customers can continue to follow their compliance program processes to meet BES Cyber Asset Reuse and Disposal requirements. (CIP-011-2 R1-R2)

### NIST CSF

**Data Security (PR.DS-3):** Assets are formally managed throughout removal, transfers, and disposition.

### Infor Responsibility

Infor use of AWS storage services including EBS, RDS, DynamoDb, and S3 encrypts data at rest and has the ability to sanitize EBS volumes, if needed. Infor controls user access to data using IAM policies and encrypt data at rest using the AWS Key Management Service (KMS). (CIP011-2, R2)

Infor is responsible for the security in the cloud and has demonstrated compliance with multiple control frameworks, addressing controls for information protection for the cloud solutions. Infor customers inherit these controls and can reference our assurance reports demonstrating the validity of our controls.

When a storage device has reached the end of its useful life, Infor' infrastructure partner AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process. (CIP011-2, R2)

Content on drives is treated at the highest level of classification per AWS policy. Content is destroyed on storage devices as part of the decommissioning process in accordance with AWS security standards. AWS hosts are securely wiped or overwritten prior to provisioning for reuse. AWS media is securely wiped or degaussed and physically destroyed prior to leaving AWS secure zones.

## CIP 013 | Supply Chain Risk Management

---

This standard purpose is to address specific cybersecurity supply chain risks. One example is the insertion of counterfeit components into cyber assets and insecure vendor manufacturing and development practices. CIP-013 and C-SCRM also aim to improve security against an increasing number of attacks that target supply chains, particularly those involving third-party providers. At-risk suppliers include hardware and software developers of BES cyber assets and BES system integrators.

The following areas should be addressed as part of Supply Chain Risk Management:

- Ensure complete and sufficient evidence of compliance
- Ensure conformance to established policies and procedures
- Prevention of inadvertent disclosures of sensitive information

## CIP 013-1 | Supply Chain Risk Management

---

### CIP Requirement

NERC CIP-013-1 purpose is “to mitigate cyber security risks to the reliable operation of the BES by implementing **security controls** for supply chain risk management of BES Cyber Systems.” To achieve its purpose, CIP-013-1 mandates responsible entities to “develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems.” These plans must be reviewed and approved every 15 months by a CIP Senior Manager.

Mandatory elements of the plan focus on software integrity and authenticity, vendor remote access to BES cyber systems, information system planning and procurement, and vendor risk management and procurement controls.

### Customer Considerations

Customers should review their compliance program processes to ensure they are complying with NERC CIP-013-1 is an important first step in safeguarding the nation’s electric infrastructure from cyberattacks that originate among supply chain vendors. Taking steps early on to ensure sustainability and developing a coherent strategy can make compliance a solid foundation upon which to establish additional tailored supply chain cyber protections.

### NIST CSF

NIST SP 800-53 standard combine elements of cybersecurity with an increased emphasis on third-party vendors and suppliers. Furthermore, NIST 800-161 specifically addresses 19 areas of supply chain risk management. The IEC/ISA 62443 standard and the SANS Institute also provide guidance focused on supply chain risk management. In line with NIST and SANS, FERC and NERC have recognized that this area also affects utilities, which now rely more heavily on third parties in their supply chains. As a result, FERC Order 829, issued in July 2016, asked for the development of a CIP reliability standard that addresses “supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations.”

### Infor Responsibility

Infor FedRAMP Authorized solutions are built on NIST CSF, that includes NIST 800-53 & NIST 800-161 which provides the assures that customers can leverage our solutions to meet CIP-013 requirements. Additionally, our approach to integrations apply the same high level security of FIPS 140-2 encryption and Transport Layer Security (TLS) to not only meet NERC CIP-013 compliance, it enables our customers to take steps to ensure sustainability and developing a coherent strategy can make compliance a solid foundation upon which to establish additional tailored supply chain cyber protections.

## CIP-014 | Declaring and Responding to CIP Exceptional Circumstances

---

The purpose of this standard is to identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

This CIP-014 (Critical Infrastructure Protection) standard provides a structured framework that is to help secure critical electrical power grid junctures from high-level physical threats and vulnerabilities in the present and future. When a ballistic barrier meets these standards, it will protect one of the largest industrial machines that is vital for both quality of life and both the local and national economy.

## CIP-014-2 R1 | Declaring and Responding to CIP Exceptional Circumstances

---

### CIP Requirement

Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection.

1.1 Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection; or
- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection.

1.2 The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

### Customer Considerations

Customers can continue to follow their risk assessment processes to protect the physical security of their facilities and control centers in order ensure that they are appropriately protected according to regulatory requirements. This includes requirements for risk assessments from an external organization, and a comprehensive incident response plan and associated training. (CIP-014-2 R1R6)

### NIST CSF

**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

**Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

### Infor Responsibility

Infor Enterprise Asset Management (EAM) solution supports the ability to perform and store results associated with risk assessments to include subsequent recommended actions to include timelines (ex: re-inspect in 1 month).

The scheduled risk assessments can be planned for execution and associated validation on a calendar basis.

## CIP-014-2 R2 | Declaring and Responding to CIP Exceptional Circumstances

---

### CIP Requirement

Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1.

### Customer Considerations

Customers can continue to follow their risk assessment processes to protect the physical security of their facilities and control centers in order ensure that they are appropriately protected according to regulatory requirements. (CIP-014-2 R1R6)

### NIST CSF

**Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

### Infor Responsibility

EAM has the ability to capture activities performed by third-party providers, to include results that may be captured during a verification assessment.

## CIP-014-2 R3 | Declaring and Responding to CIP Exceptional Circumstances

---

### CIP Requirement

For a primary control center(s) identified by the Transmission Owner according to Requirement R1, Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation verified according to Requirement R2, and b) is not under the operational control of the Transmission Owner: the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2.

### Customer Considerations

Customers can continue to follow their risk assessment processes to protect the physical security of their facilities and control centers in order ensure that they are appropriately protected according to regulatory requirements. (CIP-014-2 R1R6)

### NIST CSF

**Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

### Infor Responsibility

EAM can assist with the tracking of notifications associated with the primary controls and can be configured to initiate a notification in the form of an email, or an actionable event that could include statuses, time stamps, and system driven follow up for aging and escalation.

## CIP-014-2 R4 | Declaring and Responding to CIP Exceptional Circumstances

---

### CIP Requirement

Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following:

### Customer Considerations

Customers can continue to follow their risk assessment processes to protect the physical security of their facilities and control centers in order ensure that they are appropriately protected according to regulatory requirements. (CIP-014-2 R1R6)

### NIST CSF

**Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

### Infor Responsibility

EAM has the ability to track the association between the assets + systems, their history, and the verification of threat exercises using documented processes, result capture, notification of anomalies or follow up needed and validated sign offs.

The process steps and status updates can be provided in order to ensure visibility for key stakeholders.

## CIP-014-2 R5 | Declaring and Responding to CIP Exceptional Circumstances

---

### CIP Requirement

Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes:

### Customer Considerations

Customers can continue to follow their risk assessment processes to protect the physical security of their facilities and control centers in order ensure that they are appropriately protected according to regulatory requirements. (CIP-014-2 R1R6)

### NIST CSF

**Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

### Infor Responsibility

Using inherent capabilities, a documented process can be identified and deployed in a standardized manner. The processes may include sequential checklists, electronic signatures for signoff, and dynamic creation of follow up actions based on aging and escalation (for example, after 90 days of the 120-day allowable cycle, if no security plan has been developed, notify designated staff

### CIP Requirement

Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5.

### Customer Considerations

Customers can continue to follow their risk assessment processes to protect the physical security of their facilities and control centers in order ensure that they are appropriately protected according to regulatory requirements. (CIP-014-2 R1R6)

### NIST CSF

**Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

### Infor Responsibility

EAM can support the capture and / or storage of a third-party review evaluation.

The storage of the evaluation could be in the form of Document Management capabilities, or as an associated file linked to an event representing the evaluation and its results.





Infor builds business software for specific industries in the cloud. With 17,000 employees and over 68,000 customers in more than 170 countries, Infor software is designed for progress. To learn more, please visit [www.infor.com](http://www.infor.com).



Copyright ©2020 Infor. All rights reserved. The word and design marks set forth herein are trademarks and/or registered trademarks of Infor and/or related affiliates and subsidiaries. All other trademarks listed herein are the property of their respective owners. This document is provided for informational purposes only and does not constitute a commitment to you in any way. The information, products and services described herein are subject to change at any time without notice. [www.infor.com](http://www.infor.com).

641 Avenue of the Americas, New York, NY 10011

INFDP2331172-en-US-0620-1