Deloitte.

servicenow

ServiceNow North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Implementation Guide

October 2025

Table of Contents

Purpose

The purpose of this document is to provide Registered Entities, subject to North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards, guidance on the tools and capabilities ServiceNow offers which may be utilized to guide Registered Entities' efforts to maintain their compliance obligations while leveraging the ServiceNow cloud-based solutions.

The content provided herein is for informational purposes only. This document reflects ServiceNow offerings or practices as of the date of its publication. While this document is designed to support customers' compliance efforts, customers are responsible for making their own independent assessments of the information provided and the suitability of ServiceNow's offerings for their specific regulatory requirements. This document is not a statement of compliance or assurance, and it is not a part of, nor modifies, any agreement between ServiceNow and its customers.

Background

FERC Overview

The Federal Energy Regulatory Commission, or FERC, is an independent agency that regulates the interstate transmission of natural gas, oil, and electricity.

The Energy Policy Act of 2005 (Energy Policy Act) gave the Federal Energy Regulatory Commission (Commission or FERC) authority to oversee the reliability of the Bulk Electric System (BES), commonly referred to as the power grid. This includes authority to approve mandatory cybersecurity reliability standards.

NERC Overview

NERC is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the power grid. NERC develops and enforces Reliability Standards, annually assesses seasonal and long-term reliability, monitors the bulk power system through system awareness, and educates, trains, and certifies industry personnel.

NERC, which FERC has certified as the nation's Electric Reliability Organization, developed CIP cyber security reliability standards. NERC is the Electric Reliability Organization (ERO) for North America, subject to oversight by the FERC and governmental authorities in Canada. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. See NERC key players.

The NERC CIP Standards are a set of regulations and guidelines designed to safeguard essential services and assets that are vital to national security, public health, and safety, as well as economic stability. These standards were developed and enforced to ensure the resilience and security of critical infrastructure assets.

NERC CIP Standards are continually under review and are updated regularly. This guide addresses the following NERC CIP Reliability Standards:

Table: NERC CIP Reliability Standards

NERC CIP Reliability Standard	Purpose
CIP-002-5.1a – BES Cyber System Categorization	To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.
CIP-003-8 – Security Management Controls	To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
CIP-004-7 – Personnel & Training	To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting BES Cyber Systems.
CIP-005-7 – Electronic Security Perimeter(s)	To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
CIP-006-6 – Physical Security of BES Cyber Systems	To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
CIP-007-6 – System Security Management	To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
CIP-008-6 – Incident Reporting and Response Planning	To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.
CIP-009-6 – Recovery Plans for BES Cyber Systems	To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.
CIP-010-4 – Configuration Change Management and Vulnerability Assessments	To prevent and detect unauthorized changes to BES 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.
CIP-011-3 – Information Protection	To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

CIP-012-1 – Communications between Control Centers	To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers.
CIP-013-2 – Supply Chain Risk Management	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.
CIP-014-3 – Physical Security	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 instability, uncontrolled separation, or Cascading within an Interconnection.
CIP-015-1 – Cyber Security – Internal Network Security Monitoring	**Effective Date – 10/01/2028:** To improve the probability of detecting anomalous or unauthorized network activity in order to facilitate improved response and recovery from an attack.

NERC and the Cloud

NERC revises and updates its reliability standards requirements to meet the demands of modern computing. NERC understands that the electric utility industry is constantly evolving and transforming as technology, such as cloud, continues to evolve and innovate. However, with the opportunities to modernize BES reliability operating services (also known as BROS) come new risks that Registered Entities should consider and navigate. As more Registered Entities seek to implement cloud services, NERC seeks to update the NERC CIP requirements to allow Registered Entities to utilize cloud services. Additional information regarding deploying cloud services in a NERC CIP environment can be found in NERC's white paper on BES Operation in the Cloud and NERC's Security Guideline for the Electricity Sector - Supply Chain.

Who is ServiceNow?

ServiceNow provides both Platform as a Services (PaaS) and Software as a Service (SaaS) offerings. NERC classifies Software as a Service (SaaS) as an application that allows users to connect to and use several types of cloud-based applications over the Internet. The applications are accessible through various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure, like the one utilized by ServiceNow, including network, servers, operating systems, or storage.

ServiceNow empowers organizations, streamlines processes, improves efficiency, and reduces costs by automating tasks. Customers may access what they need, when they need it, through streamlined digital workflows. At the core of ServiceNow is the ServiceNow AI Platform, a cloud-based foundation that supports AI-powered enterprise applications for workflow automation, along with a robust database and low/no-code development tools for seamless customization. To meet diverse security and compliance, ServiceNow offers two cloud deployment options: Government Community Cloud (GCC) / Federal Risk and Authorization Management Program (FedRAMP) highly regulated industries and Commercial Cloud for standard enterprise environments.

Government Community Cloud

ServiceNow has created a separate cloud, the GCC, to meet the requirements of US Federal, State, Local, and Tribal governments as well as commercial entities with a need to protect US Federally regulated data. GCC has a Federal Risk and Authorization Management Program (FedRAMP) high authorization. This includes annual assessments by an accredited independent Third-Party Assessment Organization (3PAO) and ongoing work to satisfy the continuous monitoring requirements of the FedRAMP program. For more information on the ServiceNow GCC please see the ServiceNow FAQ.

FedRAMP authorization documentation for the GCC is available to GCC customers in the ServiceNow HiWave customer portal. GCC authorization documentation resides here: KB20003165. Prospective ServiceNow customers or ServiceNow customers not currently using GCC may be given temporary access to review GCC/FedRAMP authorization documentation in the ServiceNow FileCloud repository. Please contact your ServiceNow Account Team to arrange access.

Commercial Cloud

Registered Entities that choose not to leverage the GCC/FedRAMP environment have the option to use instances in the ServiceNow Commercial Cloud. There may be business reasons why a Registered Entity opts for the Commercial environment, including operational flexibility, offshore developers, integration preferences, or specific compliance considerations.

The ServiceNow Commercial Cloud provides secure, scalable cloud computing. To provide transparency and compliance, ServiceNow undergoes independent third-party Service Organization Control (SOC) audits, which assess its ability to meet security and compliance objectives. These reports may be utilized by entities and their auditors in understanding the controls ServiceNow has in place to support operational and regulatory requirements.

Commercial Cloud SOC Reports are available in the ServiceNow CORE Compliance Portal. CORE is a self-service documentation library supporting customers with a need to analyze the ServiceNow security program and capabilities.

Who is Deloitte?

Deloitte is a leader in cybersecurity services, serving clients in the power sectors to manage evolving cyber risks, strengthen security, meet compliance, and maintain operational reliability. Our experience with municipal, state, and commercial utilities spans grid modernization, microgrid deployment, carbon reduction, advanced technologies like internal control system (ICS), internet of things (IoT), and distributed renewables, and regulatory compliance—enabling us to address the unique needs of power companies across multiple regions. Our experience combines operational knowledge and regulatory understanding, including the NERC CIP Reliability Standards, to lead and implement cybersecurity programs that are both compliant and resilient.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to more than 75% of the Fortune Global 500® companies, including over 95% of the Fortune 1000 power and water utilities companies.

Deloitte has provided guidance to a wide range of Registered Entities across the nation and understands the requirements they should consider when meeting compliance with NERC. Deloitte is familiar with the different Regional Entities who perform audits under NERC and may guide Registered Entities in developing strategies and a security program to meet compliance, pass audits, and secure their network and the BES from malicious actors. Visit the Deloitte Energy, Resources & Industrials (ER&I) page and the Deloitte Services page for more information about what Deloitte has to offer within the power and utilities industry.

Building on its 180-year history, Deloitte spans more than 150 countries and territories across six continents. Learn how Deloitte's more than 460,000 people worldwide make an impact that matters at Deloitte's home page.

Deloitte and ServiceNow Alliance

The Deloitte and ServiceNow alliance give organizations critical tools to absorb today's continuous flow of disruptions with speed, scale, and insight.

Deloitte guides its clients and enhances business outcomes by leveraging ServiceNow as an end-to-end digital workflow platform. Deloitte does not only leverage ServiceNow to automate current processes. Deloitte also provides insight into reimagining how work gets done, delivering revenue and cost reduction.

ServiceNow is adopting a forward-thinking approach by offering products and services that may be leveraged by Registered Entities to help meet the stringent requirements set by NERC. These products leverage the ServiceNow advanced technological capabilities that may streamline compliance processes, enhance operational efficiency, and guide Registered Entities to adhere to regulatory standards. By integrating the ServiceNow AI Platform with Deloitte's recognized subject matter knowledge, organizations may benefit from a powerful combination of innovative technology and deep industry knowledge. Deloitte's experience in navigating the complexities of NERC standards provides valuable insights and practical solutions, guiding clients in their efforts to achieve and maintain compliance with confidence. Together, ServiceNow and Deloitte provide a solution that not only addresses current regulatory challenges but also anticipates future circumstances, positioning organizations for sustained success in a rapidly evolving regulatory landscape. The alliance with ServiceNow gives utilities a new avenue to create efficiencies in the way they meet compliance when working with Deloitte.

As a ServiceNow Global Elite Partner with 11+ years of experience delivering ServiceNow transformation programs, 10,500+ practitioners, 11,000+ certifications, 16 ServiceNow Certified Technical Architects (CTAs) and 13 ServiceNow Certified Master Architects (CMAs), Deloitte is recognized for collaborating with 5,500+ clients to re-architect work and unlock business value. With deep industry knowledge, Generative AI services, and distinctive capabilities spanning Deloitte's Advise, Implement, and Operate (AIO) offerings, Deloitte integrates advisory services into 6,000+ ServiceNow-led project implementations and innovation-led operations.

Speed

The average client wants value from their ServiceNow platform delivered **45% faster and on a continuous basis**. We help you implement technology in weeks.*

Scale

Clients expect solutions to scale globally to at least **300% more users and 5+ adjacent solutions**. We'll help you establish connectivity across your stakeholders and your business functions.*

Insight

90% of clients want solutions to **be sector-specific and peer leading practices**. We'll help you identify patterns within your organization and how to contextualize those patterns in your industry or domain.*

*Figures based on client experiences & Deloitte IP

Benefits of the Cloud and ServiceNow

Cloud services are a game-changing innovation that includes a broad set of public, private, and business process outsourcing capabilities with recognized scalability, redundancy, elasticity, and flexibility. Cloud services, like each major technology shift over the years, have both guided business innovation and fostered new cyber risks. Deloitte's Cloud Cyber Risk Services group has worked with various organizations across various industries for many years. Deloitte offers insights that are built upon its demonstrated delivery methodology and leverages deep technical experience, industry and regulatory knowledge, vendors, and our access to a large global network of skilled professionals.

Efforts to understand and guide cloud adoption are ongoing within NERC CIP drafting teams, which adhere to the Standards Development Process. Revisions to CIP-004 and CIP-011 helped facilitate and clarify the use of BCSI in the cloud. The standard CIP-013 requires Registered Entities to implement supply chain risk management practices to protect the BES from cyber threats, and to conduct vendor risk assessments. ServiceNow employs security measures that can be used to deny unauthorized access to BCSI, hence allowing Registered Entities to move BCSI to the cloud while maintaining compliance.

Registered Entities inherit additional security controls from ServiceNow, which adds an additional layer of security. This creates a trusted and resilient environment for Registered Entities. Through various means including encryption, continuous monitoring, and independent audits such as SOC 2 and FedRAMP annual 3PAO assessments, ServiceNow provides a secure solution for managing critical infrastructure data. By offering both GCC/FedRAMP and Commercial Cloud, ServiceNow allows entities to choose a deployment model that best addresses their security and compliance circumstances.

Together, Deloitte and ServiceNow can enhance traditional cross-departmental, back-office service delivery models by providing process standardization, automation, and operating efficiencies, without negatively impacting compliance requirements.

Security, Shared Responsibility, and Inheriting Controls

Security in the Cloud –Registered Entity Responsibility

Registered Entities are responsible for maintaining security in the cloud and the protection of their regulated assets. This includes managing the configuration of application software.

Registered Entities should carefully evaluate the products they choose, as the Registered Entity's responsibilities vary based upon the characteristics of the products themselves, how those products get integrated into their IT environments, and the applicable laws and regulations

affecting those products. Registered Entities are encouraged to work with ServiceNow account representatives regarding how to appropriately implement ServiceNow products and services.

When using ServiceNow products and services, Registered Entities maintain control over their content and are responsible for managing the configuration of their security controls, including:

- Selection of the ServiceNow products and security features used by the Registered Entity.
- The geographic location where their instances of the ServiceNow AI Platform is hosted.
- Whether their data is masked or anonymized.
- Whether their data is encrypted at rest and how encryption keys are managed. (Data encryption in transit is provided by ServiceNow AI Platform).
- Who has access to their data and how those access rights are granted, managed, and revoked, including setting up Multifactor Authentication (MFA) to manage access rights.

	Responsibility		
Area of Responsibility	**Customer**	**ServiceNow**	**Colocation (data center providers)**
Security contact details	●		
Secure configuration of instance	●		
Authentication and authorization	●		
Data management (classification and retention)	●		
Data encryption at rest	●		
Data encryption in transit	●	●	
Encryption key management	●	●	
Security logging and monitoring	●	●	
Secure SDLC processes	●	●	
Penetration testing	●	●	
Vulnerability management	●	●	
Privacy compliance	●	●	
Compliance: regulatory and legal	●	●	●
Employee vetting or screening	●	●	●
Physical security/environment controls		●	●
Cloud infrastructure security management		●	
Infrastructure management		●	
Media disposal and destruction		●	
Backup and restore		●	
Business continuity and disaster recovery		●	

This table shows areas of responsibility for ServiceNow AI Platform security.

Security in the Cloud – Inherited Controls

Registered Entities may benefit from security controls inherent in cloud infrastructure. ServiceNow's infrastructure is designed to be both flexible and secure, meeting the stringent security requirements of critical organizations, including military institutions, global banks, and power and utilities.

An example of an inherited security control is physical access controls of ServiceNow data centers. Physical access to data centers housing IT infrastructure components is restricted to authorized data center employees who require access to execute their jobs. Access to facilities is only permitted at controlled access points that require multi-factor authentication designed to prevent tailgating and only allow authorized individuals to enter a data center.

The shared responsibilities between the Registered Entity, ServiceNow, and the data center provider may provide additional levels of security for the Registered Entity. However, the Registered Entity may need to consider compliance implications when utilizing a cloud service, such as ServiceNow. The following sections provide details regarding considerations for ServiceNow products and capabilities that may be utilized to support NERC CIP compliance.

ServiceNow Vault – Platform Encryption

The ServiceNow Platform Encryption bundle comprises of two encryption products that work together to meet customers' most common circumstances:

1. **Cloud Encryption (CE)** encrypts the data within the database at the instance storage volume.
2. **Field Encryption Enterprise**, replacing Column Level Encryption Enterprise (CLEE), may then be used to encrypt selected fields or attachments at the application layer and configure what user roles may view in an unencrypted state. This is used to only allow authorized employees encrypt or decrypt specific sensitive data.

Cloud Encryption

Cloud Encryption provides block encryption of the instance storage volume that contains a ServiceNow AI Platform Instance database with industry-standard, customer-controlled, key lifecycle management, built into the ServiceNow AI Platform user interface.

Cloud Encryption encrypts data at rest in the database storage volume using symmetric AES 256-bit encryption without impacting instance functionality. Database-related activity log data (e.g., bin, redu, undo, and error) is stored within the encrypted volume.

When Cloud Encryption is enabled, cloning within the vertical instance hierarchy (e.g., production, test, and development) is fully supported. Encryption is enabled and maintained based upon the source instance's current configuration (i.e., if you clone an encrypted prod -source to an unencrypted sub prod -target, the new clone sub prod will be encrypted).

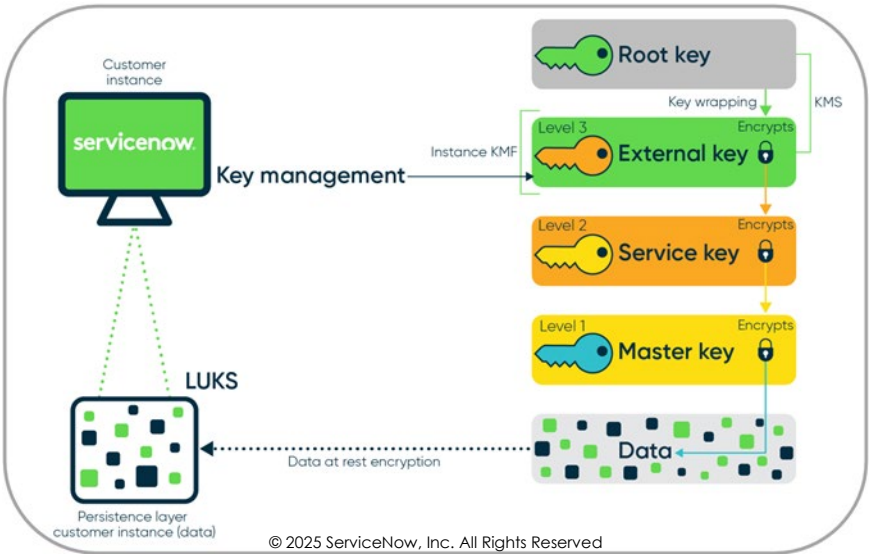
Cloud Encryption employs the Key Management Framework (KMF), which gives customers the option to use ServiceNow Managed Keys (SMK), or a key created and supplied by the customer, using the BYOK (Bring Your Own Key) capability. With either option, the key is stored by ServiceNow in a key hierarchy rooted in a FIPS 140-2 Hardware Security Module (HSM) and Key Management System (KMS) to allow the instance to be able to read, process and update data, as well as run workflows that utilize the data.

Key rotation operations are completely managed by customer admins from within their ServiceNow AI Platform instance, providing flexibility and autonomy, as well as avoiding the need to involve ServiceNow customer support.

Cloud Encryption key hierarchy

Cloud Encryption is performed using a multi-layer approach. The External key (Level 3) is the key being managed by operations provided with ServiceNow AI Platform Cloud Encryption. The External Key is stored within the ServiceNow Key Management System (KMS). The root key is embedded in a FIPS-140-2 L3 HSM. The Service Key and Master Key are stored in a secure way on the instance itself. The keys are stored and managed by ServiceNow as follows:

- **Master key – Level 1:** The Master key is a part of Linux Unified Key Setup (LUKS) that functions as the data encryption key. It includes an AES-XTS Mode key. AES-XTS requires two AES keys, each 256 bits, totaling 512 bits.
- **Service key – Level 2**: The Service key is an AES 256 bit key that provides protections for access to the Master key and is wrapped by the External key.
- **External key – Level 3:** The External key is an AES 256 bit key stored in the FIPS 140-2 validates Key Management Systems within the same ServiceNow Data Centers as the customer's instance it is associated with. This key is either a SMK (ServiceNow Managed Key) or a CMK (Customer Managed Key) provided by the customer using the BYOK (Bring Your Own Key) option.



Field Encryption Enterprise

Field Encryption Enterprise provides field-level and attachment-based data encryption within instances of the ServiceNow AI Platform. Field Encryption Enterprise is only available as part of the Platform Encryption Bundle. Field Encryption Enterprise uses the KMF encryption modules, granting customers more control of server-side encryption. Customer admins may configure which specific data fields to encrypt, within a specific table, thereby storing the data in encrypted form. Encryption keys are stored and maintained within the ServiceNow AI Platform instance and managed through the Key Management Framework (KMF). The key features of Field Encryption Enterprise are:

- Encryption of supported field types like string text, date/time fields, attachments, and URLs.
- Employs AES-CBC (Cipher Block Chaining) or AES-GCM (Galois Counter/Mode) with 256-bit keys.
- Offers both deterministic and non-deterministic encryption options.
- Allows a user with applicable access to perform limited searching and filtering operations on data that has been encrypted.
- Field Encryption Enterprise may be used on file attachments.
- Allows customers to supply their own encryption keys BYOK (Bring Your Own Key) or have keys generated on the ServiceNow AI Platform.
- Offers several access controls based on role assignment and application scope which determines if a user in the instance may decrypt data or not.

Mitigating the risk of exposing sensitive data as either the result of a direct attack or of compromised data stored in the cloud

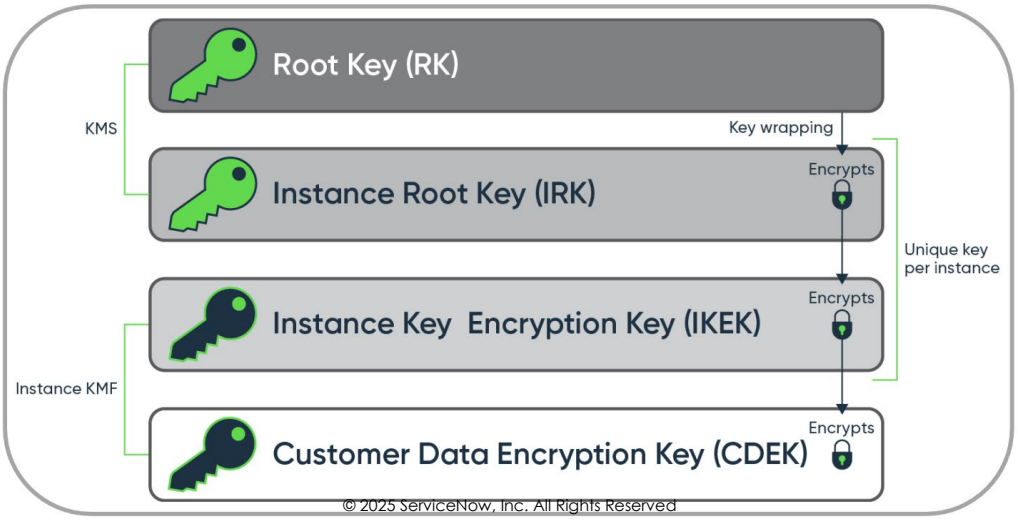
Enabling customers to comply with governmental and industry certification requirements and regulations

Limiting access to sensitive data based on defined roles, defined script assignments, application scope, and domain membership

CLE/Field Encryption Enterprise key hierarchy

Column Level Encryption (CLE) and Field Encryption Enterprise Module Keys (also known as Customer Data Encryption Key [CDEK]) use an application layer data encryption key, which is the actual key performing the encryption of specific columns within tables.

To protect the application layer data encryption key, a key hierarchy is used, protected by a root key stored within a tamper-resistant HSM that is FIPS 140-2 L3 validated.



The root key encrypts the IRK. This key is customer instance specific and stored securely within the Key Management System.

The IRK encrypts the Instance IKEK, which is stored in a secure way on the instance. The IKEK encrypts the CDEK which is also securely stored on the customer instance itself.

The keys stored on the instance are protected by the keys stored in the KMS and HSM, this approach leverages the concept of a "hardware root of trust."

To provide availability of the keys there are HSM's in each data center pair within a data center region.

Encryption keys provided by customers for use with Field Encryption Enterprise are backed up within the database for the customer instance where they are used. Customers should also back up encryption keys prior to supplying them to their instances.

Note: Field Encryption Enterprise does not enable customers to store encryption keys in their own HSMs, key storage appliances, or services.

More information about cloud encryption and encryption key management with ServiceNow may be found within the ServiceNow Data Encryption White Paper.

NERC CIP Compliance in the Cloud

Customer Responsibility Considerations

The following sections discuss considerations regarding the NERC CIP Standards that may be enhanced by cloud services. Whether data is housed on-premises or in the cloud, Registered Entities should implement proper data handling procedures and controls to protect NERC CIP data and assets.

With the implementation of cloud services, the Registered Entity should consider how the evidence generation and compilation processes may differ from on-premises. NERC uses the

Evidence Request Tool (ERT) to document evidence for various security domains as they relate to the NERC CIP Reliability Standards. Additionally, NERC and Regional Entities may request Registered Entities to use Reliability Standard Audit Worksheets (RSAWs) or NERC's Align and Secure Evidence Locker (SEL) to document their compliance processes and evidence. While the processes of submitting evidence to Regional Entities may not change with the implementation of cloud services, Registered Entities should consider how cloud services may impact their processes to demonstrate compliance.

Access Management and BES Cyber System Information (BCSI) Security

Although ServiceNow implements safeguards and security controls for the cloud platform, including the physical and electronic protection of servers that house BCSI, Registered Entities are responsible for implementing access controls and managing data security within their cloud instance. It is the entity's responsibility to enforce role-based access, encrypt data at rest, and securely delete information when no longer needed.

CIP-004 (Personnel and Training) and CIP-011 (Information Protection) outline specific requirements for managing personnel access to BES Cyber Assets and BCSI, as well as the classification and protection of sensitive information. The Registered Entity must implement controls to restrict access, secure data at rest and in use, and comply with audit retention policies, deleting evidence once no longer required.

ServiceNow facilitates the secure destruction of data storage media, following CIP-011's media protection requirements, through a third-party destruction service. This process is performed within the data center under the supervision of ServiceNow Data Center Services. A certificate of destruction is provided as verification.

Network Security

Registered Entities are responsible for implementing instance security hardening. Per CIP-005 (Electronic Security Perimeters), Registered Entities must establish secure network boundaries around their BES Cyber Assets and enforce secure access controls. Although ServiceNow encrypts data in transit, the Registered Entity is responsible for securing inbound and outbound communications at the Electronic Security Perimeters.

System Security Management

CIP-007, System Security Management, requires Registered Entities to implement technical, operational, and procedural controls to protect BES Cyber Systems from compromise that could impact grid stability. This standard covers multiple security areas that must be addressed when utilizing cloud services like ServiceNow.

Under requirement one (R1), Registered Entities must manage the ports and services used within the cloud environment, allowing only required virtual ports to reduce the attack surface.

Requirement two (R2) mandates that Registered Entities keep software associated with ServiceNow products updated with the latest patches. Patches and updates should be assessed before deployment to systems connected to the BES to prevent unintended disruptions.

Requirement three (R3) requires Registered Entities to implement mechanisms to deter, detect, and prevent malicious code. This includes using traditional antivirus solutions, application whitelisting, network isolation techniques, and Intrusion Detection/Prevention Systems (IDS/IPS) to strengthen BES Cyber Assets against cybersecurity threats.

Under requirement four (R4), Registered Entities must log and generate alerts for detected security events, such as successful and failed login attempts, access violations, and malicious code detections. Entities are responsible for monitoring traffic to and from the cloud and logging and analyzing security events.

Finally, requirement five (R5) requires Registered Entities to control system-level access and maintain an inventory of accounts and users. When utilizing cloud services that store BES Cyber System Information, Registered Entities must implement the same level of access control as they may implement for on-premises BES Cyber Assets to implement proper security and compliance.

Incident Response and Recovery

CIP-008, Incident Reporting and Response Planning, requires Registered Entities to identify, classify, and respond to cybersecurity incidents. Entities must manage and respond to incidents involving data stored in the cloud and malicious activity originating from or targeting cloud services. Effective incident response plans must be implemented to analyze and mitigate threats before they impact the BES.

CIP-009, Recovery Plans for BES Cyber Systems, mandates that Registered Entities create and implement recovery plans to maintain the stability, operability, and reliability of the BES in the event of a cybersecurity incident. Under the shared responsibility model, ServiceNow is responsible for data backups and restoration within its cloud environment, providing data integrity and availability. However, Registered Entities must maintain recovery procedures for on-premises cyber assets that interact with cloud services, providing disaster recovery and business continuity planning.

Configuration Change Management and Vulnerability Assessments

CIP-010, Configuration Change Management and Vulnerability Assessments, requires Registered Entities to establish and maintain configuration baselines for applicable BES Cyber Assets. Registered Entities must document these baselines, including cloud services related to operating systems, firmware where no independent operating system exists, commercially available or open-source application software, custom-installed software, logical network-accessible ports, and applied security patches.

When utilizing cloud services, Registered Entities should analyze that configurations affecting BES Cyber Assets remain aligned with security and compliance requirements. ServiceNow supports this process by maintaining a secure and controlled cloud environment, while the Registered Entity remains responsible for tracking, documenting, and managing configuration changes that impact their systems.

ServiceNow provides Registered Entities with the ability to automate and generate reports from the change control process, supporting the Registered Entity with demonstration of compliance with CIP-010. This automation reduces manual effort, improves accuracy, and creates an environment where required documentation is readily available for audits and regulatory reviews.

Third Party Risk Management

CIP-013, Supply Chain Risk Management, requires utilities to identify, assess, and mitigate cybersecurity risks associated with their supply chains for BES Cyber Systems. Registered Entities must create and implement documented supply chain risk management plans that address procurement and contract management processes. This standard seeks to safeguard against third-party products and services introducing vulnerabilities into the BES, strengthening the overall security and reliability of critical infrastructure. These requirements should be carefully considered when evaluating cloud services and their associated providers.

While adopting cloud services may introduce new NERC CIP compliance considerations, they may also enhance a Registered Entity's compliance posture by providing automation, visibility, and risk management capabilities.

Internal Network Security Monitoring

As of September 2024, the FERC issued a Notice of Proposed Rulemaking (NOPR) to approve CIP-015-1, Internal Network Security Monitoring. Starting on October 1st, 2028, Registered Entities will have to implement Internal Network Security Monitoring (INSM) for high-impact BES. 24 months after the effective date, Reinserted Entities will have to implement the INSM for medium-impact BES with ERC as part of NERC's phased-in implementation. Once enforced, Registered Entities will be required to monitor and protect internal network security within the Registered Entity's Electronic Security Perimeter(s).

When utilizing cloud services, the Registered Entity's role in complying with the CIP-015 standard remains the same as when utilizing non-cloud services. The Registered Entity will need to monitor network traffic inside the Electronic Security Perimeters in the cloud.

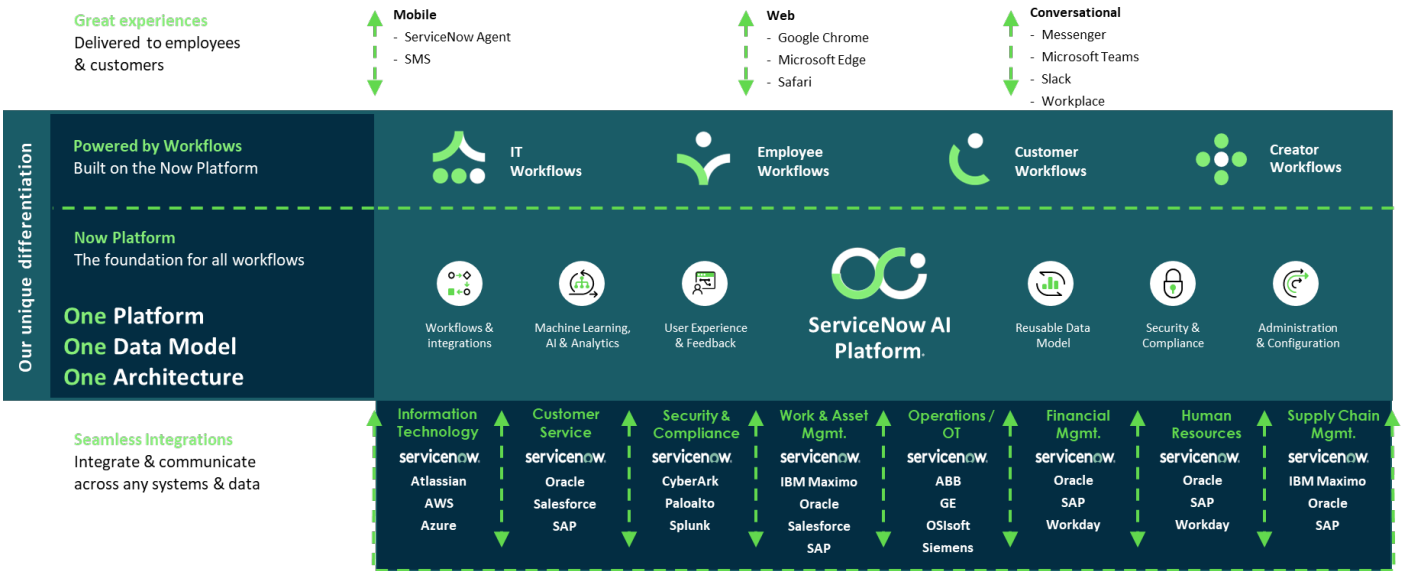
ServiceNow Capabilities

This section focuses on the ServiceNow products and services that Registered Entities can use to help achieve compliance needs. This ranges from tools providing overarching compliance management services to tools with specific uses, such as encryption key management services.

ServiceNow offers the Audit Management product, which prioritizes internal audits using risk data and entity-specific information to reduce recurring audit findings, enhance audit assurance, and increase productivity.

ServiceNow offers the Governance, Risk, and Compliance (GRC) product to provide customers with an integrated approach that builds operational resilience and mitigates risk. The GRC product spark action to address compliance and privacy issues, business disruption, third-party risks, and cybersecurity threats across the enterprise. By utilizing the Integrated Risk Management module, a utility may improve visibility and risk-related decisions with real-time intelligence and increase productivity and reduce costs with automated workflows across your enterprise to guide the GRC strategy.

Additionally, ServiceNow offers products to centralize a Registered Entity's security approach. ITOM Discovery may be utilized to get visibility across your cloud, containerized, on-premises, and hybrid infrastructure. Improve accuracy with a single system of record and action. The Integration Hub product may be utilized to connect modern systems quickly with ServiceNow to accelerate productivity. Use AI to reduce costs, complexity, and risk as you simplify process



automation throughout the enterprise. The APIs and Integration Tools product may be utilized to integrate and automate ServiceNow with system or data with APIs and low-code solutions.

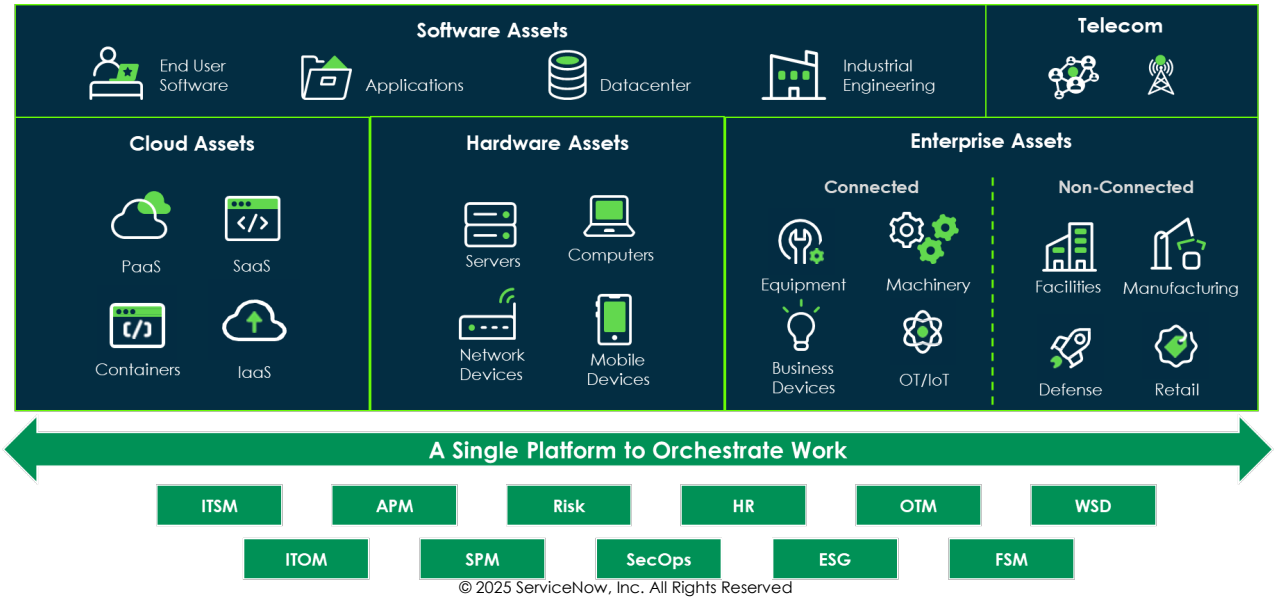
Governance and Asset Categorization

The CIP-002 Standard, BES Cyber System Categorization, focuses on the identification, categorization, and documentation of a Registered Entities BES Cyber Systems and applicable BES Cyber Assets. The implementation of a specific BES Cyber Asset inventory is only required for High and Medium Impact BES Cyber Systems; however, an inventory of Low Impact BES Cyber Assets may be utilized to improve the security of Low Impact BES Cyber Systems.

ServiceNow offers the ability to manage assets and oversee infrastructure, operations, and field services as part of its Asset Management Core product. Additionally, ServiceNow offers the IT Asset Management product to manage hardware, software, and cloud IT assets from a single platform. The Registered Entity may automate stages of the IT asset lifecycle at scale while controlling costs and minimizing licensing and leasing risks. The Registered Entity may utilize ServiceNow to manage the asset lifecycle process and maintain a single source for inventory of BES Cyber Assets. Additionally, as further discussed in the "Training and Identity Access Management" section, ServiceNow products may be utilized to manage access to the lifecycle and inventory of BES Cyber Assets.

ServiceNow offers the Asset Management Core and IT Asset Management products that may be utilized by the Registered Entity to manage the lifecycle of BES Cyber Assets. As part of the review that must be performed at least once every fifteen calendar months, the Registered Entity may utilize ServiceNow to update and review the inventory with applicable personnel and maintain an up to date and single source of truth for their BES Cyber Asset inventory and categorization.

ServiceNow offers the Enterprise Asset Management (EAM) meant to automate the full lifecycle of physical business assets with prescriptive workflows across functions to increase productivity, improve the useful life of assets, and reduce costs and risks at scale. The EAM product may be used to streamline the review process and track actions that may have impacted specific BES Cyber Assets over the previous fifteen calendar months. This visibility allows Registered Entities to analyze changes, investigate their impact on asset categorization, and maintain compliance with regulatory requirements. By leveraging EAM, utilities may enhance asset tracking, maintenance, and governance, to secure critical infrastructure and document its information.



Training and Identity Access Management

CIP-004, Personnel and Training, focuses on personnel with access to BES Cyber Systems and BES Cyber System Information are properly vetted, trained, and managed. This standard is divided into two specific areas: personnel requirements and access management.

The personnel requirements mandate that individuals undergo security training before being granted access to BES Cyber Systems. This training provides and overview so that authorized personnel understand their responsibilities, security risks, and compliance obligations.

The access management component requires Registered Entities to implement authentication, authorization, and revocation processes to control access to BES Cyber Systems and information. This includes analyzing user identities, assigning applicable access levels, and promptly revoking access when no longer required. Proper implementation of these controls is used to protect critical infrastructure from unauthorized access and potential security threats.

ServiceNow cloud personnel are required to complete a criminal background check and participate in a security training program. Upon commencement of the employment process, prospective candidates undergo particular background checks and screening, which include criminal, employment, financial, and government watch list checks. As a condition of employment, personnel must sign a non-disclosure agreement and confirm their understanding of the ServiceNow Code of Conduct and Ethics policy, as well as the Acceptable Use Policy. Personnel complete annual security awareness Training. The training content includes insider threats, and social engineering attacks and is updated yearly to address emerging security topics, risks, and threats.

Personnel Requirements

ServiceNow offers the Employee Journey Management product to provide personalized cross-departmental employee journeys with intelligent workflows that provide guidance for in-moment tasking, learning, and listening. The Registered Entity may utilize this product to assign new hires and existing employees with required regular security awareness training, recurring cyber security training, and Personnel Risk Assessments (PRA). ServiceNow offers automated workflows that may be used to track when personnel last completed their training requirements and PRA and send reminders notifying personnel of upcoming renewal deadlines.

ServiceNow offers the HR Service Delivery (HRSD) product to improve productivity by making it easy for employees to get the guidance they need, in one place. This product may be utilized to give personnel easy access to commonly asked questions about employee requirements and find help when completing required actions.

Access Management

NERC CIP requires Registered Entities to manage the access to applicable BES Cyber Systems and BES Cyber System Information (BCSI). While ServiceNow is not a dedicated Identity Access Management (IAM) solution, Registered Entities may integrate and automate ServiceNow with system or data with Application Programming Interfaces (APIs) and low-code solutions using the APIs and Integration Tools product which support various inbound and outbound API authentication methods including Open Authorization (OAuth), API Key, and manual Transport Layer Security (mTLS). By utilizing ServiceNow, the Registered Entity may track both their inventories and the access to BES Cyber Assets and BCSI and create automated workflows to manage access, create access requests tickets and track employee requirements for authorized access (i.e., cyber security training, PRAs, and business need). By integrating tools, ServiceNow workflows may be used to remove access as well. NERC CIP has requirements to revoke access to applicable BES Cyber Systems and BCSI within 24 hours of an individual's termination action. Utilizing ServiceNow workflows may give applicable personnel the notifications they need to complete tasks to remove an individual's access. By bringing multiple

tools together and integrating them with ServiceNow, the Registered Entity may reduce administrative burden and improve the workflow for access management.

ServiceNow offers the Access Analyzer, an application that may be utilized to gain visibility into what's controlling access to a particular resource. Using Access Analyzer, organizations may improve their security posture, strengthen their compliance levels, and make configuration changes to provide the right users and groups with applicable access while preventing unintended access to sensitive data. By selecting a user, group, or role within a ServiceNow instance, organizations may evaluate what access controls are in place for a given resource, most commonly a table. This allows them to understand which access controls are applied to a user for a given resource, how access controls are evaluated and in what order, and why access is granted or denied for individual resources. Organizations may choose to report on the results, modify group and role membership, and/or modify access controls. Additionally, organizations may evaluate intended access versus granted access to align with least privilege principles, remediate access security inquiries or incidents, and properly design and test access controls on the ServiceNow AI Platform.

ServiceNow offers multiple IAM services to manage access to the ServiceNow AI Platform, including the management of user, role, group, and profile management and provisioning. ServiceNow has an access management framework including role-based access controls and attribute-based access controls to manage authorization of personnel. Additionally, ServiceNow offers authentication services to manage local logins (users and password logins), single sign-on (SSO) with external identity providers using Security Assertion Markup Language (SAML), and OpenID Connect (OIDC) open standards. The ServiceNow AI Platform supports various MFA methods such as one time password (OTP), code-generator apps, Fast Identity Online (FIDO), biometric, and various policies such as adaptive authentication.

Electronic Security

CIP-005, Electronic Security Perimeters, CIP-007, System Security Management, CIP-015, Internal Network Security Monitoring, require each Registered Entity to implement Electronic Security Perimeters (ESP) to electronically protect applicable BES Cyber Systems and manage system security. The ServiceNow configuration management database (CMDB) may track and document Cyber IT/OT/Telecom Assets within the defined ESPs. Network diagrams and asset lists may be maintained to meet compliance with ESP requirements.

The ServiceNow Security Center may be utilized by the Registered Entity for the following:

- Improving the security and compliance of your ServiceNow AI Platform instances
- Getting guidance to configure security controls and monitor potentially insecure behaviors
- Hardening system security
- Monitoring system security events and user activity

Registered Entities have administrative control over their ServiceNow instance, patch levels, modules being utilized, and encryption levels in place.

ServiceNow may enforce and document access permissions for inbound and outbound traffic through firewall rules and access control lists, managing access controls. Using the Firewall Audits and Reporting product, Registered Entities may gain visibility into their firewall policies. The product may be utilized to configure firewall rules to meet the Registered Entities policies and guide the audit process when providing evidence of firewall configurations.

ServiceNow Vault offers the ServiceNow Zero Trust Access product that may be utilized to implement least-privilege access controls and improve their security posture with continuous trust verification and security inspection of users, devices, apps, and data. With continuous trust verification and security inspection, Zero Trust Access makes it so that Registered Entities may manage network connections form employees, contractors, and third parties to be through

trusted networks and compliant devices. This proactive approach minimizes exposure to cyber threats, enhances compliance with NERC CIP requirements, and provides greater visibility into who is accessing critical infrastructure. By leveraging the ServiceNow Zero Trust Access product, organizations may align with industry leading practices for identity and access management while maintaining security and operational efficiency.

ServiceNow offers the AntiVirus Scanning product to protect the integrity of your applications and detect file-security gaps and compromises by utilizing ServiceNow antivirus tools.

Registered Entities also benefit from the electronic security controls that ServiceNow uses to protect its data centers.

Physical Security

CIP-006, Physical Security of BES Cyber Systems, and CIP-014, Physical Security, require each Registered Entity to implement documented physical security plans that outline measures such as access controls, logging, and monitoring of authorized and unauthorized access, and conducting risk assessments to evaluate potential physical security threats. These plans are used to protect critical infrastructure from physical threats that could impact the reliability of the Bulk Electric System.

The ServiceNow configuration management database (CMDB) provides a centralized system to track and document BES Cyber IT, OT, and Telecom assets within defined Physical Security Perimeters (PSP). By leveraging the CMDB, Registered Entities may maintain in-depth records of their physical security plans, and confirm that controls are implemented, monitored, and regularly updated.

ServiceNow workflows may be used by Registered Entities to efficiently manage service requests related to the development of physical security perimeters and their associated documentation. The platform may also facilitate tracking visitor access requests and logging, as well as coordinating the testing and maintenance of Physical Access Control Systems (PACS).

Additionally, ServiceNow automated workflows may be used to document and track physical security risk assessment processes, so that Registered Entities may meet the compliance requirements of CIP-014. By streamlining these processes, ServiceNow enhances visibility, accountability, and operational efficiency in managing physical security risks.

ServiceNow offers the APIs and Integration Tools product to integrate and automate ServiceNow with system or data with APIs and low-code solutions.

Incident Response

CIP-008, Incident Reporting and Response Planning, requires each Registered Entity to implement an Incident Response Plan, assess and prepare for potential cyber security incidences. ServiceNow offers the Event Management product to replace event noise with insights and clarity driven by generative AI (GenAI). The product may be utilized to identify issues before they may affect users, with simple, actionable alerts. Additionally, ServiceNow offers the Incident Management product to facilitate communication between personnel to track and fix issues in order to restore services and resolve problems quickly.

Recovery Management

CIP-009, Recovery Plans for BES Cyber Systems, requires Registered Entities to create and implement recovery plans to maintain the reliability and resilience of BES Cyber Systems in the event of an incident or disruption. These plans must outline procedures for restoring critical systems, maintaining operational stability, and allow for BES Cyber Assets to be quickly recovered to reduce impact on the Bulk Electric System.

ServiceNow offers Inventory Management that may be utilized by a Registered Entity to source and track field technician trunk stock, including swaps and transfers, managing the availability

of critical components needed for recovery. By maintaining the integrity of personal stock inventory, Registered Entities may efficiently manage the spare parts required for recovery efforts.

Additionally, the ServiceNow Business Continuity Management (BCM) solution allows customers to automate recovery workflows to meet compliance with NERC CIP-009. With BCM, Registered Entities may document, assess, and execute recovery plans, track inventories, and streamline response efforts in a structured and auditable manner. By leveraging these capabilities, organizations may enhance their ability to maintain system reliability while easily demonstrating compliance with regulatory requirements.

Configuration Change Management

CIP-010, Configuration Change Management and Vulnerability Assessments, requires Registered Entities to track the configuration baselines of Cyber Assets, conduct vulnerability assessments, and manage the use of transient cyber assets and removable media. These requirements focus on controlling, documenting, and analyzing changes to BES Cyber Systems for potential security risks to maintain system integrity and compliance.

The ServiceNow Configuration Management Database (CMDB) provides a centralized solution for maintaining and tracking the baseline configurations of BES Cyber Systems. By leveraging CMDB, Registered Entities may document system configurations, monitor changes, and analyze that updates align with compliance and security policies.

ServiceNow also provides out-of-the-box change management workflows to evaluate, approve, and document configuration changes. These workflows may guide Registered Entities to enforce structured change control processes, making it so that modifications to BES Cyber Assets are carefully reviewed and tracked for auditability.

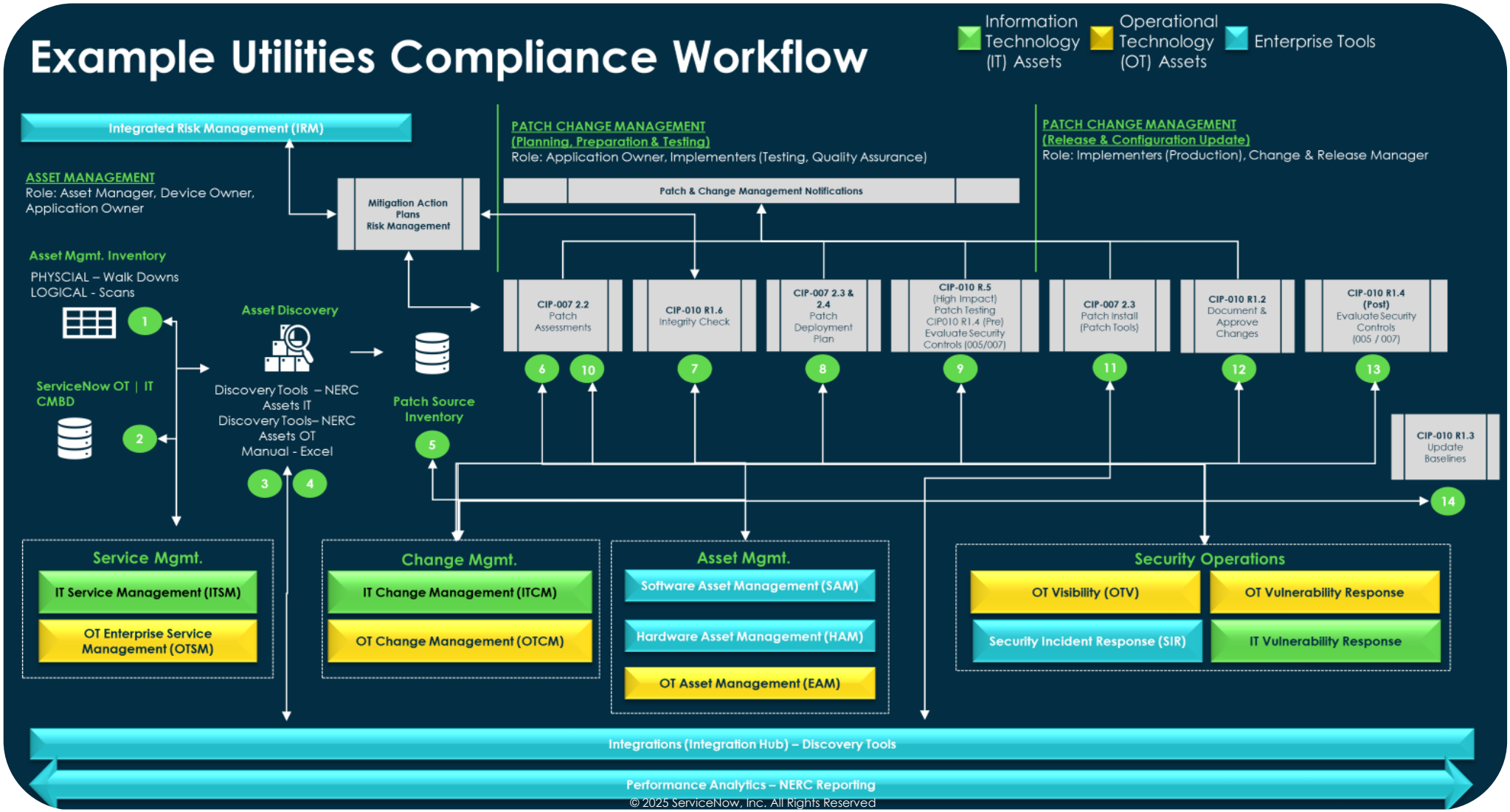
To further assist with CIP-010 compliance, ServiceNow offers additional asset management solutions:

- Hardware Asset Management (HAM) may be utilized by Registered Entities to govern Cyber Assets through prescriptive workflows and a native CMDB, guiding proper asset tracking and lifecycle management.
- Software Asset Management (SAM) may be utilized by Registered Entities to track, manage, and enhance software usage, to meet compliance with security policies and reducing software-related vulnerabilities.
- Enterprise Asset Management (EAM) provides a full lifecycle management solution for BES Cyber Assets, streamlining maintenance and operational tracking to manage system reliability.
- Telecom Network Inventory Management offers visibility and governance for Telecom and 5G equipment to document and maintain infrastructure components supporting BES Cyber Systems.

By integrating these solutions, ServiceNow helps Registered Entities to automate and streamline configuration change management processes and meet their compliance with CIP-010.

The following page is an illustrative example workflow demonstrating how ServiceNow may be utilized by Registered Entities to meet compliance.

The following is an example workflow demonstrating how ServiceNow may be utilized by Registered Entities to meet compliance.



Information Protection

CIP-011, Information Protection, focuses on protecting the confidentiality, integrity, and availability of BES Cyber System Information (BCSI). It requires utilities to identify information that requires protection, establish methods to secure it, and only allow for authorized individuals to have applicable access. Additionally, the standard mandates the development of procedures for the destruction or reuse of media containing sensitive information to prevent unauthorized disclosure. This makes it so that critical infrastructure information remains secure against cyber threats.

ServiceNow document management capabilities may be used to maintain and track documentation related to BES Cyber System Information. Configurable access controls help Registered Entities restrict and monitor access to BES Cyber System Information stored within the ServiceNow AI Platform.

ServiceNow offers the Vault product to help protect BCSI that resides on ServiceNow products and increase security, privacy, and compliance across the enterprise. Vault groups a set of premium security and privacy controls into a scalable package that may grow as your circumstances change.

Vault consists of five services:

1. Platform Encryption:

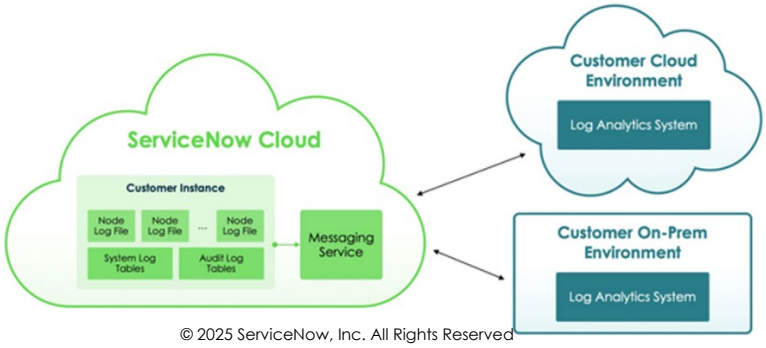
Platform Encryption offers critical solutions to help protect data at rest or in-app. The Platform Encryption subscription bundle includes two types of encryption- **Cloud Encryption** and **Field Encryption Enterprise**. The Key Management System offers options, including the ability to use customer-supplied keys through the Bring Your Own Key (BYOK) feature.

2. Data Privacy:

ServiceNow Data Privacy offers a framework including Discovery and Classification tools to allow organizations to manage and protect personal and sensitive data throughout its lifecycle, meeting compliance with data protection regulations and standards such as California Privacy Rights Act (CPRA), General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and others. Additionally, ServiceNow Vault provides powerful Data Discovery and Data **Anonymization** capabilities, allowing organizations to redact sensitive information within their instances, particularly useful for GDPR's "right to be forgotten" requirements.

3. Log Export Service:

The ServiceNow Log Export Service (LES) allows for simple exporting of instance system and application logs to enterprise security analytic tools. LES leverages Hermes Messaging Service, which is built on Apache Kafka, which enables the instance to produce and consume large volumes of Kafka events. The external log analytic systems, either in the cloud or on-prem, may use and consume the log events from the Hermes Messaging Service.

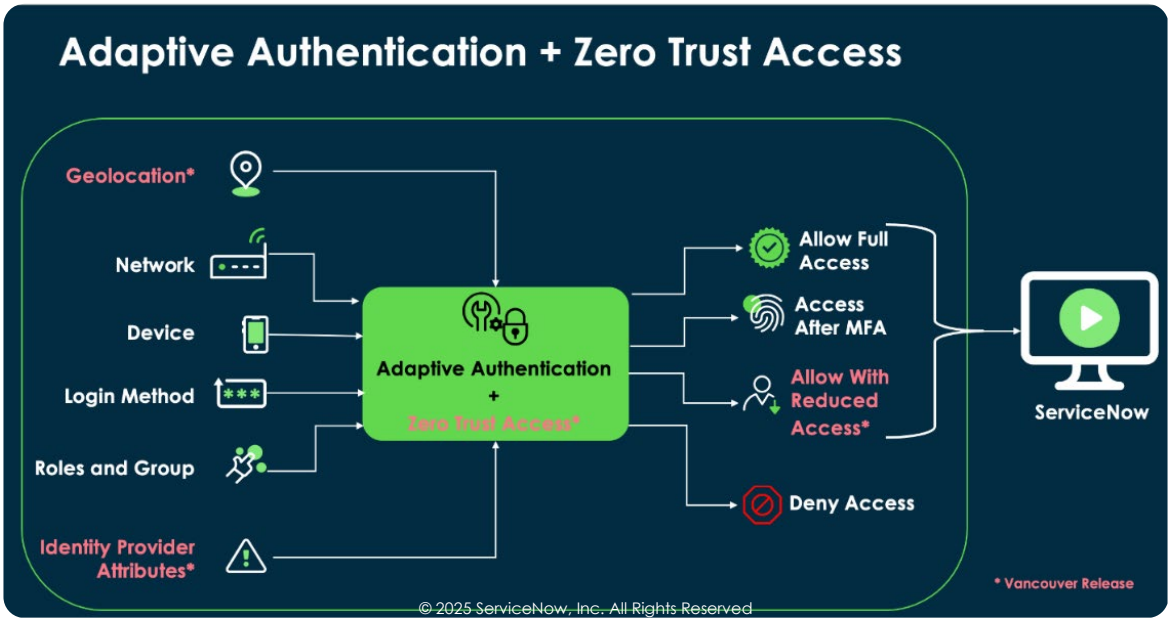


4. Code Signing:

ServiceNow Code Signing enhances security by testing sensitive application configuration data and scripts before they are used. This process involves creating digital signatures for the data, analyzing the data's authenticity and integrity.

5. Adaptive Authentication + Zero Trust Access:

Zero Trust Access allows security administrators to create contextual policies that define the user's access level based on factors such as network, location, authentication method, and identity provider attributes. This allows organizations to dynamically reduce user privilege in a web session based on a variety of factors, including IP address, location, authentication method, user's role, group, user having MFA and attributes shared by the Identity Provider (IDP). This may help to protect organizations from unauthorized access and data breaches, even when high-privileged users access applications from untrusted devices or locations.



With Vault the Registered Entity may implement platform encryption to safeguard your sensitive data and integrate ServiceNow system and application logs into your enterprise security analytics. Additionally, Vault utilizes ServiceNow Zero Trust Access to implement adaptive access rules to respond to rapid changes in identity risk. Additionally, ServiceNow offers ServiceNow Platform Encryption product to protect your sensitive data. The ServiceNow Platform Encryption product is comprised of a free of cost/out of box Field Encryption Enterprise and a premium ServiceNow Vault Cloud Encryption product that may be utilized to protect sensitive data at

scale and use an intuitive key management framework. The products may be used to create, rotate, and revoke keys automatically.

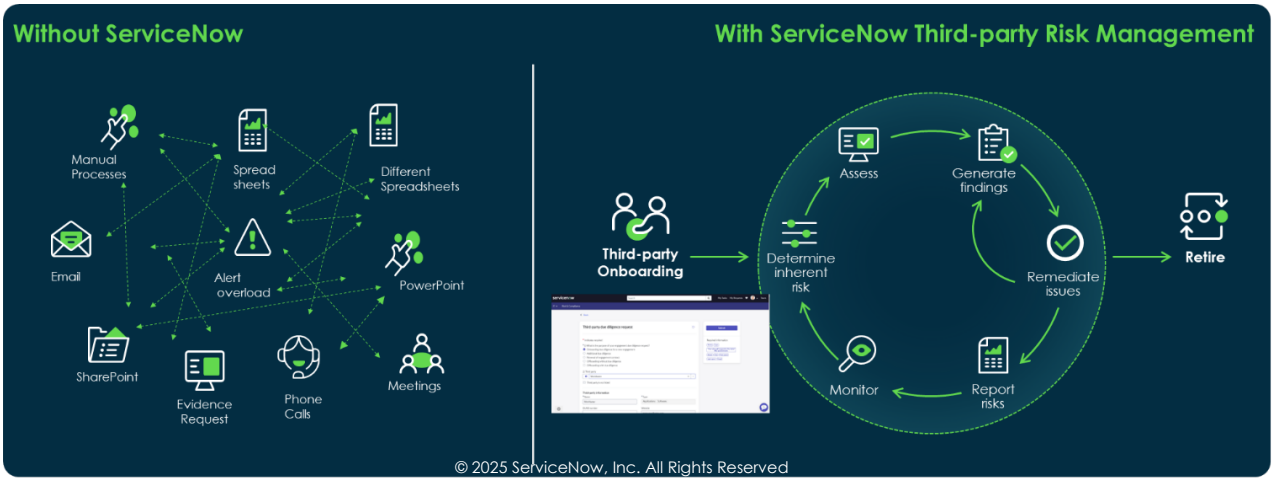
Communication Between Controls Centers

CIP-012, Communication between Control Centers, requires Registered Entities to protect the confidentiality, integrity, and availability of Real-time Assessment and real-time monitoring data transmitted between Control Centers. While ServiceNow is not a dedicated tool to analyze the real-time communication between Control Centers, Registered Entities may integrate and automate ServiceNow with system or data with APIs and low-code solutions using the APIs and Integration Tools product.

Supply Chain Risk Management

CIP-013, Supply Chain Risk Management, requires Entities to direct cyber-related procurements for the BES through applicable supplier and supply chain cyber risk management processes. This compliance is crucial to reduce the risk of missed procurements that could potentially compromise the security and reliability of the BES. ServiceNow offers Third Party Risk Management that may be implemented with risk assessments to guide Registered Entities in evaluating several critical factors to determine the inherent risk associated with their procurements. These factors include:

- Cyber Threat: The potential for malicious actors to exploit vulnerabilities in the procurement process or the products and services being procured.
- Technology Risk: The risks associated with the technology being procured, including its lifecycle, compatibility with existing systems, and potential for obsolescence.
- Manufacturing and Development: The risks related to the processes and practices of the manufacturers and developers of the procured technology, including their security measures and quality control practices.
- Network Security: The ability of the procured technology to integrate securely within the existing network infrastructure to avoid the introduction of new vulnerabilities.
- Platform and Data Security: The measures in place to protect the integrity and confidentiality of data on the procured platform, including encryption, access controls, and data loss prevention mechanisms.



Upon determining the inherent risk through these assessments, Registered Entities may then establish the required steps for escalation, mitigation activities, and approvals. Escalation involves bringing the identified risks to the attention of higher management or specialized teams for further analysis and decision-making. Mitigation activities are the actions taken to reduce the identified risks to an acceptable level, which may include implementing additional security controls, changing suppliers, or modifying procurement specifications. Finally, obtaining the

required approvals makes it so that risk management activities are documented and authorized by the relevant stakeholders, thereby maintaining accountability and compliance with CIP-013 standards. By following these risk management processes, Registered Entities may enhance the security and resilience of the BES against cyber threats.

Appendix 1: ServiceNow Mapping to NERC CIP Standards

NERC CIP Requirement	ServiceNow Module	Description
CIP-002: BES Cyber System Categorization	Policy and Compliance Management; CMDB (Configuration Management Database)	Guides in identifying and categorizing BES Cyber Systems based on their impact on the Bulk Electric System. The CMDB provides a centralized repository for tracking and managing configuration items (CIs) and their relationships.
CIP-003: Security Management Controls	Policy and Compliance Management; Risk Management; Security Incident Response	Guides in establishing and maintaining security management controls and policies. This includes creating, implementing, and monitoring security policies, analyzing, and managing risks, and responding to security incidents.
CIP-004: Personnel & Training	Vendor Risk Management; Policy and Compliance Management; HR Service Delivery	Manages personnel training to meet compliance with security training requirements. HR Service Delivery tracks training schedules, completion status, and may be used to train personnel with access to BES Cyber Systems.
CIP-005: Electronic Security Perimeter(s)	Risk Management; Policy and Compliance Management; Security Operations (SecOps)	Guides in defining and managing electronic security perimeters and associated access controls. SecOps provides continuous monitoring and management of security events and incidents.
CIP-006: Physical Security of BES Cyber Systems	Risk Management; Policy and Compliance Management; Facilities Management	Manages physical security controls and compliance for BES Cyber Systems. Facilities Management supports the development and enforcement of physical security policies to restrict and monitor physical access to critical systems.
CIP-007: System Security Management	Risk Management; Policy and Compliance Management; Vulnerability Response; IT Operations Management (ITOM)	Guides in managing system security controls, including patch management and vulnerability assessments. ITOM may be used to manage regular updates, identify, and mitigate vulnerabilities, and maintain security controls.
CIP-008: Incident Reporting and Response Planning	Incident Management; Policy and Compliance Management; Security Incident Response	Facilitates incident reporting, response planning, and management of security incidents. This module supports the creation of incident response plans, and tracks incidents from detection to resolution.
CIP-009: Recovery Plans for BES Cyber Systems	Business Continuity Management; Policy and Compliance Management; IT Service Continuity Management (ITSCM)	Supports the development and maintenance of recovery plans for BES Cyber Systems. ITSCM may be used to create, test, and update recovery plans to prepare for quick and effective restoration of critical systems in the event of a disruption.
CIP-010: Configuration Change Management	Change Management; Vulnerability Response; Policy and Compliance Management; IT	Manages configuration changes and conducts vulnerability assessments to meet compliance. This module tracks system configuration changes, assesses impacts, and guides the

and Vulnerability Assessments	Operations Management (ITOM)	prompt identification and mitigation of vulnerabilities.
CIP-011: Information Protection	Policy and Compliance Management; Risk Management; Security Incident Response; Data Loss Prevention (DLP)	Guides the protection of sensitive information related to BES Cyber Systems. DLP may be utilized to create and enforce information protection policies, conduct risk assessments, and secure the handling and storage of sensitive information.
CIP-013: Supply Chain Risk Management	Vendor Risk Management; Policy and Compliance Management; Procurement Management	Manages risks associated with the supply chain for BES Cyber Systems. Procurement Management may be utilized to analyze and manage risks posed by third-party vendors, to meet compliance with security policies, and monitors vendor performance and compliance.
CIP-014-3 – Physical Security	Risk Management; Policy and Compliance Management; Facilities Management	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 instability, uncontrolled separation, or Cascading within an Interconnection.
CIP-015-1 – Cyber Security – Internal Network Security Monitoring	Risk Management; Policy and Compliance Management; Security Operations (SecOps)	**Effective Date – 10/01/2028:** To improve the probability of detecting anomalous or unauthorized network activity in order to facilitate improved response and recovery from an attack.