COGNITE

Cognite Data Fusion® Support for NERC CIP v.5

Cognite Data Fusion® Support for NERC CIP v.5

Table of contents

Introduction ..... pg. 3
- Background ..... pg. 3
- Applying NERC CIP V. 5 ..... pg. 3

Cognite Data Fusion® ..... pg. 4
- Cognite Data Fusion® solution security ..... pg. 4
- Defense in depth ..... pg. 4
- Secure by design ..... pg. 4
- Shared responsibility ..... pg. 5
- Data security and access control ..... pg. 5
- Resilience ..... pg. 6
- Cognite Data Fusion® alignment to NERC CIP v.5 ..... pg. 6

Appendix: Cognite Data Fusion® alignment to NERC CIP v.5 ..... pg. 7

About Cognite

Cognite is a global industrial SaaS company that supports the full-scale digital transformation of asset-heavy industries around the world. Our core Industrial DataOps platform, **Cognite Data Fusion®**, enables data and domain users to collaborate to quickly and safely develop, operationalize, and scale industrial AI solutions and applications.

Cognite Data Fusion® codifies industrial domain knowledge into software that fits into your existing ecosystem and enables scale from proofs of concepts to truly data-driven operations to deliver both profitability and sustainability.

WHY COGNITE DATA FUSION® → BENEFITS FOR YOUR TEAMS → CONTACT SALES →

Introduction

Background

The North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) compliance program was established in 2008. The NERC CIP standards were developed to ensure that those operating assets in North America's Bulk Electric System (BES) maintain security controls to protect electricity infrastructure and its customers from cyberattacks, cybervandalism, or acts of cyberterrorism. NERC CIP requires utility companies in North America to establish and adhere to a baseline set of cybersecurity measures. The NERC CIP standard includes 12 control areas currently enforced for BES Operators:

- CIP-002-5.1a BES Cyber System Categorization
- CIP-003-8 Security Management Controls
- CIP-004-6 Personnel & Training
- CIP-005-6 Electronic Security Perimeter(s)
- CIP-006-6 Physical Security of BES Cyber-Systems
- CIP-007-6 System Security Management
- CIP-008-6 Incident Reporting and Response Planning
- CIP-009-6 Recovery Plans for BES Cyber-Systems
- CIP-010-3 Configuration
- Change Management and Vulnerability Assessments
- CIP-011-2 Information Protection
- CIP-013-1 Supply Chain Risk Management
- CIP-014-2 Physical Security

While NERC CIP is a regulatory requirement for bulk power system operators, solution and service providers like Cognite play an important role in contributing to and sustaining the security posture and the program compliance of power and utility operators. This paper evaluates how Cognite Data Fusion® aligns to and supports customer compliance to NERC CIP v.5.

NERC CIP V. 5

The US electric sector is regulated by the Federal Energy Regulatory Commission (FERC). FERC has regulatory responsibility for interstate transmission of liquefied natural gas, oil, and electricity. In 2006, FERC named the North American Electric Reliability Corporation (NERC) as the Electric Reliability Organization (ERO). NERC, in turn, gained the authority to develop Critical Infrastructure Protection (CIP) cybersecurity reliability standards that support security and reliability of grid planning and operations. BES operators and owners must demonstrate that they meet the defined Bulk Electric System scope, and they are mandated to comply with the NERC CIP standards for the data, assets, and systems in-scope of the standards. NERC CIP V.5 is a standard that evolves with the electricity industry.

As cloud computing and virtualization gain greater interest and adoption among BES operators, regulators have recognized the opportunities that cloud technology offers to enhance reliability in the sector. Importantly, the NERC CIP standards also recognize that the needs of Bulk Electric System Cyber System Information (BCSI) are different from BES cyberassets. BES cyberassets are those that could impact reliable operations within 15 minutes of interruption in service, such as a Supervisory Control and Data Acquisition Systems (SCADA) or Energy Management Systems (EMS). Industry approved revisions to CIP-004 and CIP-011 now enable and clarify use of BES Cyber System Information (BCSI) in the cloud in alignment with a NERC Practice Guidance. While still pending FERC approval, this revision enables CIP auditors in assessing BCSI in the cloud in advance of the requirement revisions. The revisions are pending FERC approval. In June 2019, NERC endorsed guidance to rely on a third party's independent assessment as an acceptable means of identifying and assessing risk (CIP-013-01).

Cognite Data Fusion®

Cognite is a SaaS provider, and Cognite Data Fusion® is our industrial DataOps platform product. We also offer subscription-based access to configurable business applications.

Cognite Data Fusion® streams data into **the CDF data model**, where the data is normalized and enriched by adding connections between data resources of different types and stored in a graph index in the cloud. With your data in the cloud, you can use services and tools in Cognite Data Fusion® to build solutions and applications to meet your business needs.

With Cognite, you own your data. We use your data only to provide agreed-upon services. We handle your data **securely**, and we comply with privacy and legal regulations. If you leave our services, Cognite ensures that customers maintain data ownership.

You can interact with your data through the portal application, or work with the data with our **API and SDKs.**

Cognite Data Fusion® solution security

As more industries that rely on operational technology adopt cloud technology, it's critical to apply robust and more automated cybersecurity risk management practices for each interconnected system to protect the confidentiality, integrity, and availability of data. Cognite Data Fusion® integrates with existing equipment and infrastructure to provide insights and realize value from your industrial data. To fulfill our responsibility as a trusted custodian, we have developed and implemented the Cognite security commitment: a set of principles focusing on people, processes, and technology that inform the design and operation of Cognite Data Fusion®.

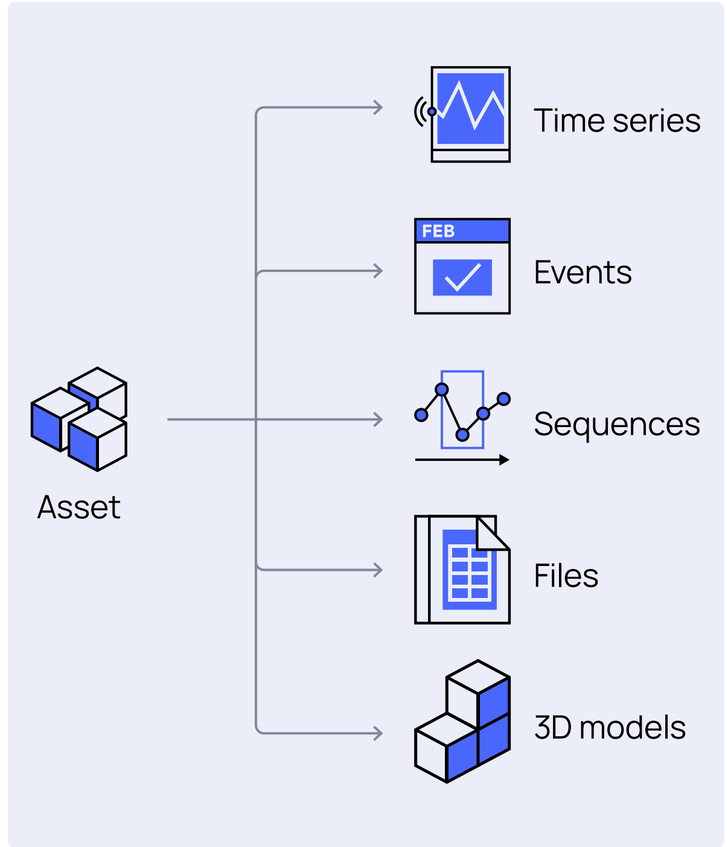
Defense in depth

Cognite operates in mission critical, asset-heavy industries where operational technology security is table stakes. With Cognite Data Fusion®, security is a collaboration between the customer, Cognite, and cloud provider (for example Microsoft or Google).

Cognite supports defense in depth through:

- Industry security compliance and regulations
- Secure development life cycle
- Security logging and monitoring
- Incident response

Security stakeholders are critical to the successful scaling and sustaining of Industry 4.0 programs. We welcome the opportunity to engage and support security stakeholders.



Secure by design

- Meeting product standards: Cognite's management system (QMS and ISMS) is ISO 9001 and ISO 27001 certified. The operation and data processing in Cognite Data Fusion® comply with the

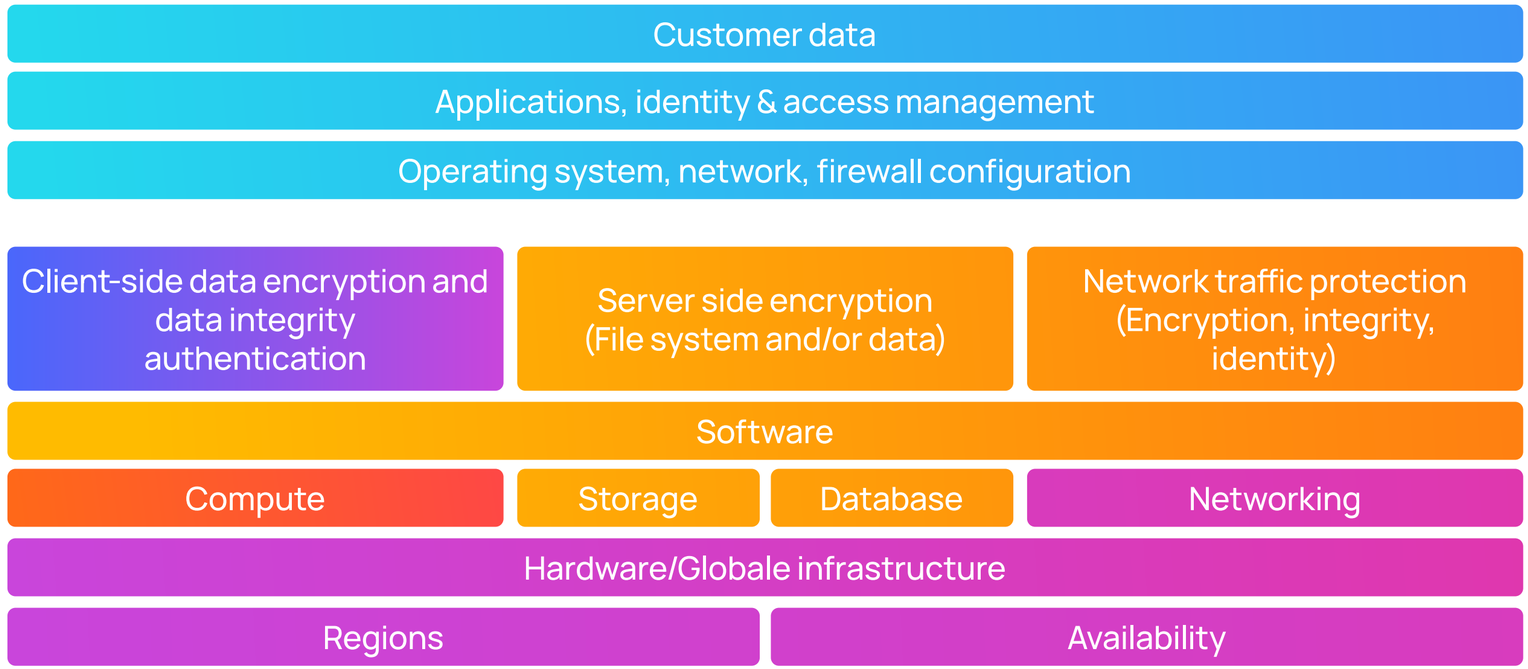
WHY COGNITE DATA FUSION® → BENEFITS FOR YOUR TEAMS → CONTACT SALES →

General Data Protection Regulation (GDPR).

- Secure development life cycle: Cognite invests in security awareness and training to support integrated DevSecOps practices. Security practices supported with: (1) a comprehensive audit and observability stack, (2) test and security automation (2), and a robust incident response process and practices.

- Least privilege and access control: Customers control access to data through integration using their organization's identity provider. Within Cognite project engagements, privileged access to customer data is strictly limited and role-based.

- Secure data: Encryption at rest and in transit.



Shared responsibility

The shared responsibility model is fundamental to understanding the respective roles of the context of the cloud security principles. This model identifies ownership across the customer organization, Cognite, and the customer's cloud service provider (CSP).

Cognite's world-class CSP partners are responsible for infrastructure composed of the hardware, software, networking, and facilities that run cloud services.

Cognite maintains a strong relationship with CSPs to use platform and infrastructure security controls that comply with industry standards. These processes, procedures, and tools support the strong security foundation of Cognite Data Fusion®. As new technologies and threats emerge, Cognite is uniquely positioned to take advantage of these security updates in its products.

Customers retain control of the security program that they choose to implement to protect their content, applications, systems, and networks. Cognite supports data encryption in transit and at rest in collaboration with CSP. Cognite holds responsibility for the application's secure development lifecycle and associated vulnerability management.

Data security and access control

- Access control. Customer-defined users, roles, and privileges, as structured in the customer's identity provider (IdP), determine how access control to customer data is managed. Cognite employees' access to customer data is granted via the IdP, and the customer can choose when to enable and revoke that access.

- Data security. Encryption in transit: Data owner/source, Cognite APIs, and traffic internal to Cognite Data Fusion® are encrypted with TLS 1.2 and higher.

  Encryption at rest: Server-side encryption using cloud service-managed keys for encryption and decryption.

Cognite controls in place to prevent data leakage or intentional or accidental compromise include:

- Data encryption with cloud service provider (CSP) encryption key
- Customer controlled data access: integration with customer's identity provider (IdP) service. Requests and API calls are mapped to roles and permissions from the IdP.
- Principle of least privilege and changes managed in code with approval (peer-review) flow.
- Network and infrastructure policies that control and restrict access to only authenticated or authorized services.
- Logical separation inside shared data stores.
- CSPs use cryptographic authentication and authorization at the application layer for inter-service communication.
- CSPs rely on ingress and egress filtering throughout the network to prevent IP spoofing as a further security layer.

Resilience

Cognite Data Fusion® is built on cloud infrastructure configured to be highly available. Deployment is continuous and incremental with smaller changes to minimize impact and potential for disruption, while ensuring the ability to quickly validate or confirm changes. Cognite routinely performs testing of business continuity and disaster recovery plans (tabletop and real exercises) that validate scenarios and functionality including confidentiality, integrity, and availability.

Specific security controls supporting NIST 800-61 standard guidelines to support detection, response, and recovery include: Incident handling processes guided independently certified compliant to ISO 9001 and 27001.

Preparation: Processes and tools in place and continuous improvement through applying lessons learned.

Containment: Organizing and limiting or preventing damage.

Eradication: Eliminate root cause and prepare for system restore.

Recovery: Bring systems back to production in desired state and monitor.

Cognite Data Fusion® alignment to NERC CIP V. 5

As a SaaS solution, Cognite Data Fusion® maintains management best practices supporting customer alignment and compliance to NERC CIP v.5. Appendix 1, which follows, provides detailed context on how Cognite Data Fusion® supports BES owner and operator compliance to relevant control areas.

Appendix: Cognite Data Fusion® alignment to NIST CSF

Description	CIP Requirement ID	Cognite Support of Control
BES Cyber System Categorization	CIP-002-5.1a-R1	Cognite assets associated with information and information processing facilities are inventoried and classified throughout the respective life cycles. The inventory is documented and maintained in an inventory system, which provides an accurate and up-to-date inventory through new installations, changes, and decommissioning of assets.
Communications Between Control Centers	CIP-012-R1	Cognite is not a registered entity and is not responsible for this requirement.
Configuration Change Management and Vulnerability Assessments	CIP-010-2-R4	Cognite's Acceptable Use Policy and Bring Your Own Device Policy govern the overall use of information, electronic data, computing devices, and network resources. The policies prohibit the use of Cognite's information systems or assets in a manner that is deliberately malicious or detrimental to their security, performance, capacity, or integrity, or that poses a threat or liability to either Cognite, its employees, its customers, or the public at large.
	CIP-010-2-R3	The Cognite Security Audit Logging and Monitoring Policy defines required monitoring for infrastructure, services, accounts, and logging for vulnerabilities and irregular activities. Cognite uses industry-standard third-party tools and custom-built tools and solutions that provide reporting data based on a number of existing industry-accepted open standards. These tools itemize software flaws, security configurations, and various product names, including asscoiated Common Vulnerabilities and Exposures (CVE). Cognite uses internal and third-party security specialists and auditors to test, evaluate, and audit operations and environments on a regular basis. Issues and vulnerabilities that are reported or detected are logged, tracked, and prioritized. Prior to changes being implemented, information security and business impact analysis is performed and reviewed. Changes are analyzed as part of the standard change process, both prior to and after implementation, to verify that modifications provided the expected output. All items have a named owner, priority, management visibility, and tracking.

Description	CIP Requirement ID	Cognite Support of Control
Configuration Change Management and Vulnerability Assessments	CIP-010-2-R1	Cognite follows the secure software development lifecycle (SSDLC) to govern the design, development, deployment, and maintenance of all CDF services. This includes reviews of and updates to configuration settings and baseline configurations of hardware, software, and network. Changes are developed, tested, and approved prior to being introduced into the production environment from development or test environments. Baseline configurations are documented, managed, and maintained along with the source code control repositories. Prior to being introduced, impact analysis is performed and reviewed by each service team. Changes to baseline configurations go through the SSDLC process, which requires relevant sign-offs prior to production readiness and deployment. Cognite's Change Management Policy brings discipline and quality control throughout the life cycle. Cognite practices continuous integration and continuous delivery (CI/CD) through breaking down significant changes into subcomponents. This discipline reduces the chance of changes causing problems and enables more rapid detection and resolution when needed. When changes are executed, the process is recorded, classified, and documented in an automated tracking and logging system. Change management is supported by design documents, code review, testing, and approval. For significant or breaking changes, the project management process handles the announcement and communication. Affected users are notified prior to such a change being implemented. A roll-out plan is executed with provision, if any failure should occur.
	CIP-010-2-R2	Cognite uses a system to manage its infrastructure and source code changes. This system logs changes and requires users input critical log critical information (for example metadata, date, identity of requestor, and contents of change). The source code control repository contains system and service source code, and evidence of approvals and version changes. The source code repository tools provide auditing capabilities to ensure logging of changes to the baselines and configuration changes. Source code repository tools track the identity of individuals who check code out, the time of the change, and changes made to identified files. In addition to the use of automated tooling and monitoring, Cognite executes an annual review of the change management process. As part of the review, random samples of changes are selected and reviewed to ensure consistent implementation and adherence to the the change management process. This process ensures that no unauthorized changes are made to baselines. Cognite's change management process is part of Cognite's management system and is subject to external certification and attestation.

Description	CIP Requirement ID	Cognite Support of Control
Electronic /Security Perimeter	CIP-005-5-R1 CIP-005-5-R2	Cognite's security posture is deny by default, allowing only connection and communication necessary for system operation, blocking all other ports, protocols, and connections by default. External connections are managed at the system boundary using the cloud service providers' boundary protection devices and technologies. Connections within the boundary are managed using service mesh, IP filtering, and firewalls. Cognite uses a layered architecture to protect services and data. By default, only connections and communications necessary for service operation are enabled; nonnecessary ports and connections are blocked by default. Cognite's cloud service providers deliver load balancers and firewalls, while service proxies help isolate deployments at the network level. This layered approach provides a combination of broad (nongranular) protections as well as granular service-to-service level control and observability. Customers must authorize Cognite before remote access is granted. Before service team personnel can connect remotely, they must first be approved for remote access by an authorized Cognite manager. Users are identified via two-factor authentication based on a unique identifier and password from the customer's environment. The remote session uses encryption to prevent information disclosure. Customers are required to provide users with privileged or elevated access to cloud production systems for platform troubleshooting and maintenance.

Description	CIP Requirement ID	Cognite Support of Control
Incident Reporting and Response Planning	CIP-008-5-R1	Cognite's Incident Management Policy provides organization-wide guidance on proper response to, and efficient and timely reporting of, service and security incidents. The policy governs how Cognite ensures that support resources are focusing on the issues that have the greatest urgency and potentially the greatest impact on the business. The control and management information provided by this process provides Cognite's management with decision support required to prioritize resources for managing risks to Cognite achieving the company objectives. Cognite uses the CI/CD method of development to restore normal service operation as quickly as possible and to minimize the adverse impact on business operations, thereby ensuring that the best possible levels of service quality and availability are maintained.
	CIP-008-5-R2 CIP-008-5-R3	Cognite tests and verifies incident-response methodology and tools on a regular basis (at least annually) to ensure optimal performance during incidents. Testing is executed in both test and production environments. A comprehensive production and live fire exercise is conducted quarterly to validate the efficacy of methodology and tools. All results are documented and logged. Cognite monitors infrastructure, services, accounts, and logs for vulnerabilities and irregular activities using industry-standard third-party tools and custom-built tools and solutions. Cognite uses internal and third- party security specialists and auditors to test, evaluate, and audit operations and environments. Issues and vulnerabilities that are reported or detected are logged, tracked, and prioritized. All issues and vulnerabilities logged have a named owner, priority, management visibility, and progress tracking. Cognite Security conducts incident response testing and exercises per established protocols and procedures as part of the external validation layer. Relevant summaries or reports include findings and status updates. Following an incident, a formal incident postmortem report is produced by the service teams with direct engagement with Cognite's Quality and Reliability, and Security teams. These reports, which include lessons learned, are created for all events. Incident reports are maintained and provided to the relevant stakeholders for review. On a monthly basis, all incidents from the previous month are reviewed with Cognite's leadership team, with detail on (1) impact and resolution of the incident and (2) changes to the Incident Response Plan. Cognite's Incident Response Plan is revised to address system and organizational changes and challenges encountered during plan implementation, execution, or testing.

Description	CIP Requirement ID	Cognite Support of Control
Information Protection	CIP-011-2-R1 CIP-011-2-R2	Data in transit is protected using TLS (Transport Layer Security) 1.2 or higher to ensure data confidentiality as it moves between Cognite Data Fusion® and the customer. TLS provides strong authentication, message privacy, and integrity. Data at rest is protected using AES-256 CSP default encryption and cloud service provider-managed keys. Physical and logical access is restricted through identity repository security group membership in the domain where the server resides. Data residency restrictions are enabled by default and scoped based on established geographies.
Personnel & Training	CIP-004-6-R4	Cognite has established internal policies and processes to support the delivery of Cognite Data Fusion® services to customers. These internal policies are developed in consideration of legal and regulatory obligations to define Cognite's organizational approach and system requirements. Cognite's Code of Conduct and the Cognite Management System defines employee and contractor responsibilities regarding confidentiality, data protection, appropriate use of Cognite's equipment and facilities, and practices expected by the organization. Cognite uses cloud provider IAM (Identity and Access Management) to provide authentication, authorization, and access control for an organization's users, groups, and objects. The identity repository uses role-based access control (RBAC) to grant granular access to resources. Multifactor authentication (MFA) is used to secure access to sensitive information and minimize risk of malicious attack.
	CIP-004-6-R2	Cognite administers annual company-wide cybersecurity awareness and training programs to educate Cognite personnel on security basics and recent trends in security and privacy. This training reinforces expected cybersecurity practices for personnel with authorized electronic access to cloud-based resources. Additionally, prior to authorizing information system access or assigning privileges to perform newly assigned duties, as Cognite provides individual and role-based security training. Employees with access to sensitive information receive periodic reminders of their responsibilities and engage in ongoing updated security awareness training to ensure awareness of current threats and corresponding security practices to mitigate such threats. Cognite community engagement in incident simulations and exercises are used to reinforce responsibilities consistent with Cognite's policies and procedures. Electronic records of training are retained by Cognite's security group to ensure compliance to industry standards.

Description	CIP Requirement ID	Cognite Support of Control
Personnel & Training	CIP-004-6-R3	Following applicable laws and regulations. Cognite's People & Strategy department conducts background checks and enforces the screening policies for all personnel (including contractors and vendors). Aligned with applicable laws and regulations, screening and background checks are conducted for new hires or personnel transferring to positions that involve potential access to customer data. Background verification includes relevant privacy, protection of personally identifiable information, and employment-based legislation. Screening, disclosure, and retention of information (seven years) is coordinated by Cognite's People & Stratetgy department. The process is described in Cognite's Employee Background Verification Policy and is part of the Cognite Management System.
	CIP-004-6-R5	Cognite's Human Resources Security Policy covers employees, contractors, and other third-parties with clearly defined responsibilities associated with initial employment, changing roles, and termination of employment. Cognite uses internal procedures to effectively manage departing employees and the withdrawal of assigned responsibilities for employees, contractors, and other third-party users. Access rights to information and information systems are removed upon termination of employment or contractual relationship. Cognite has an established and logged procedure for the withdrawal or modification of access rights for departing employees, contractors, and third-party users. These rights are managed through the master Human Resources (HR) system and revised in the identity management (IDM) system. Changes in responsibilities and duties within Cognite include removal of all rights associated with prior roles and duties, and addition or creation of rights appropriate to the new roles and duties. Removal or reduction of access rights prior to the termination is performed where appropriate.
	CIP-004-6-R1	An information security awareness program has been established in line with Cognite's information security policies and relevant procedures, given the information to be protected and the controls implemented to protect the information. Cognite's awareness program is updated regularly to align with Cognite policies and procedures, and is built on lessons learned from security incidents.

Description	CIP Requirement ID	Cognite Support of Control
Physical Security	CIP-014-2-R1 CIP-014-2-R2 CIP-014-2-R3 CIP-014-2-R4 CIP-014-2-R5 CIP-014-2-R6	Cognite is not a registered entity and is not responsible for this requirement
Physical Security of BES Cyber Systems	CIP-006-6-R3	Cognite's cloud service providers ensure that all access control devices are inventoried at least annually. Moreover, access control devices in data centers are linked to the physical security system where device status is monitored continuously with testing and auditing according to defined policies. Such systems are part of the cloud service providers certifications (for example ISO) and attestations (for example SOC 2). If an access control device stops working, a device malfunction alert is issued immediately.
	CIP-006-6-R1	Cognite's Access Control Policy defines the requirements for boundary layers, physical access control, and authorization for access to Cognite premises. The policy is part of the Cognite Management System and subject to regular audit, attestation, and certification. Cognite is using CSP data centers to deliver Cognite Data Fusion® and related services. Cognite's cloud service providers enforce strong physical access control and audited authorizations for all physical access points to data centers. Please refer to the links below for the most up-to-date details and documentation. The exteriors of the data center buildings are nondescript and do not advertise that they are data centers. Depending on the design of a data center, physical access authorizations may begin at a controlled perimeter gate or secured facility door that require either access badge authorization or security officer authorization. Microsoft Azure: https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security Google Cloud Platform: https://cloud.google.com/security https://cloud.google.com/security/infrastructure

Description	CIP Requirement ID	Cognite Support of Control
Physical Security of BES Cyber Systems	CIP-006-6-R2	Cognite and Cognite's CSPs have rigorous physical security control programs including perimeter, boundaries, and personnel requirements. Visitors are only allowed at approved sites and then further only in approved areas. Visitors are required to show valid identification, have a sponsor or escort, and wear visitor badge or identification at all times. Escorted visitors do not have any access levels granted and can only travel on the access of their escorts. Escorts monitor all activities of their visitors. Record retention and auditing is conducted according to established policy and legal and regulatory requirements.
Recovery Plans for BES Cyber Systems	CIP-009-6-R2	Cognite conducts both quarterly routine disaster response exercises and, on an ongoing basis, disaster responses exercises for new services before they are put into production. Disaster response exercises are designed to test larger parts of the Business Continuity Plan. Test results are then used to plan the next cycle, supporting implementation of lessons learned and a continuous improvement approach. A full retest of disaster response capabilities is performed when major changes are made to services or underlying infrastructure. An example of a comprehensive Business Continuity Plan verification includes testing a scenario in which a cloud service provider experiences a regional outage and all services must be relocated to a different region.
	CIP-009-6-R3	Cognite's Business Continuity Plan and disaster recovery documents and plans are reviewed on an annual basis or when required to address (1) changes to the organization, information system, or operation environment; and (2) problems encountered during plan implementation, execution, or testing. Such review and revision ensure that the information included in the documents is accurate and updated. Evidence of review is captured. The Quality and Reliability team, in conjunction with Cognite's service teams, reviews supporting evidence and identifies improvement opportunities for short-, medium-, and long-term implementation. If critical issues are identified during an exercise, they are worked on until they are resolved, and related contingency plans are updated.

Description	CIP Requirement ID	Cognite Support of Control
Recovery Plans for BES Cyber Systems	CIP-009-6-R1	Cloud service providers' Disaster Recovery Plans (DRP) provide detailed processes for contingency planning of related cloud infrastructure. These documents serve as a guide for cloud service providers to respond, recover, and resume operations during a serious adverse event. The DRP cover key personnel, resources, services, and actions required to continue critical technology processes and operations. The plans are intended to address extended service disruptions. Data storage and processing takes place inside identified cloud service provider regions and corresponding data centers. Data and system configuration (infrastructure as code) is backed up based on type with frequency, retention, and restore aligned with SLA. Backup operation is verified through both alerting on errors observed and Business Continuity operations. Backup integrity is tested through Disaster Response scenario exercises. Cognite's Data Retention, Archiving, and Destruction policy identifies principles for retaining and destroying specified categories of data. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory, or contractual obligations. Disposal of records is carried out in accordance with relevant retention and disposal schedules. Confidential information is destroyed using methods which make reconstruction of the contents impossible. Archived documents are retained for seven years. Approved destruction methods appropriate for each type of information are required. Proper digital media and computer hard drive disposal methods include, but are not limited to, destroying electronic media by shredding, incineration, melting, or pulverizing.
Security Management Controls	CIP-003-7-R3 CIP-003-7-R4	Cognite's CISO is responsible for reviewing and modifying security documents and policies. Cognite maintains a delegation of authority policy that enables senior managers to delegate authority at levels which are considered appropriate to management in fulfilling its responsibilities. In exercising this authority, employees are responsible for their actions and are accountable for their decisions.
	CIP-003-7-R2	Cognite has implemented the following cybersecurity plans that can be shared upon customer request: security awareness training, incident response, disaster recovery, and vulnerability management.
	CIP-003-7-R1	Cognite's Security Policy applies to all processes and information used to conduct business. Cognite's Management System is certified against ISO 9001 and ISO 2700, which outline security training, controls, and incident response. Cognite's Management System is reviewed annually by independent auditors and in scope for the SOC 2 Type 2 attestation report. Security policies for cloud service providers are reviewed prior to and during engagement.

Description	CIP Requirement ID	Cognite Support of Control
Supply Chain Risk Management	CIP-013-1-R3	Cognite reviews all security policies and procedures on an annual basis in line with Management System attestation and certification requirements.
	CIP-013-1-R1 CIP-013-1-R2	Cognite's Supplier Relationships Security Policy ensures that information security objectives are established for third parties providing components for Cognite Data Fusion® solutions. Cognite exercises due diligence to gain a comprehensive understanding of supplier information security process and controls. Arrangements with suppliers that involve accessing, processing, storing, communicating, or managing Cognite information, information systems, or information processing facilities are based on formal agreements which contain necessary security requirements. Third-party suppliers are reviewed based on classification and planned use. Reviews result in one of three outcomes: (1) acceptable, (2) request for improvement, or (3) vendor or solution not acceptable. Sources used for supplier review include ISO certifications, SOC 2 Type 2 reports, supplier-provided documentation (including VAPT reports), standard industry certifications, and questions and answers from interviews

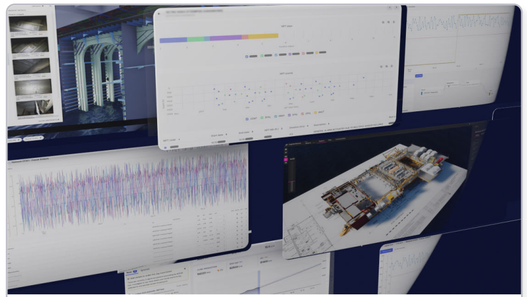
Description	CIP Requirement ID	Cognite Support of Control
System Security Management	CIP-007-6-R2	Cognite Data Fusion® is a SaaS platform with no planned downtime or patch installations. Vulnerability detection and remediation are continuously executed. Vulnerability management covers activities including network scanning, container scanning, configuration scanning, and penetration testing. Scanning is used to detect and remediate vulnerable dependencies and exposed secrets. Findings are evaluated and ranked, and mitigation activities are agreed upon with system owners and developers. Issues and bugs are tracked, and noted as open, until they have been mitigated. Changes are tested and deployed using an automated CI/CD process that enables roll back (or forward fixing) within minutes if server metrics, request logs analysis, or support tickets indicate a problem. Static application security testing (SAST) is part of the CI/CD pipeline and is a prerequisite to production release approval. Cognite also relies on dynamic application security testing (DAST) in security penetration tests for both authenticated and unauthenticated requests.
	CIP-007-6-R5	Identity management and user access follows the established shared responsibility pattern. Customers are responsible for managing the end-user accounts that interact with and use the Cognite services. This ensures alignment with customer policies and existing procedures related to (including) joining, moving, and leaving. Cognite is responsible for managing the identity and role-based permissions of personnel operating the Cognite services, including but not limited to software development and infrastructure operations. Policies and processes include onboarding and offboarding (account creation and termination) as well as permission adjustment (role change and move). Changes are managed as code using established change management processes and audit trail. Cognite's cloud service providers manage the identities and role-based permissions of personnel operating the underlying cloud infrastructure. Cloud service provider process and procedure is subject to certification and attestation; reports are available upon direct request to the relevant cloud service provider.

Description	CIP Requirement ID	Cognite Support of Control
System Security Management	CIP-007-6-R1	The Cognite cloud service infrastructure (including networks and resources) is purpose-configured with secure baseline configuration. Infrastructure is managed as code with strong change management and audit trail, and continuous monitoring of configuration and posture. Cognite manages connections at the system boundary using cloud service provider networking boundary protection devices like IP filtering and firewalls. Cognite also uses third-party tools to detect configuration issues and observe network connectivity between Cognite Data Fusion® container workloads. Cognite continuously monitors API activity, network traffic, running workloads, and to alert on anomalous behavior and known threats.
	CIP-007-6-R3	Cognite and contracted cloud service providers use a multilayered approach to protecting the cloud infrastructure and services against malicious software. Controls include the use of inventory systems, granular role-based access control with activity logging, antimalware software, and the use of cloud-native protection (immutable infrastructure) that includes scanning and behavior detection capabilities. These layers form the principal mechanism for the protection of cloud assets from malicious software and activities are further supported by operational capabilities and plans. These defensive technical measures, combined with the ability to observe, enables detection and prevents the introduction of computer viruses, malware, rootkits, worms, and other malicious software into the service systems. Cognite requires all software update testing related to flaw remediation to follow a documented change management process. Testing of possible changes to the environment are conducted to assess possible impacts to security and operations of the system. Testing must be conducted prior to approval and is a prerequisite to releasing to the production environment.

Description	CIP Requirement ID	Cognite Support of Control
System Security Management	CIP-007-6-R4	Cognite uses a combination of logging and monitoring security tooling from third-party vendors, the cloud service provider, and tools developed in-house to protect Cognite Data Fusion® at the service and platform level. Expert manual reviews occur on a regular basis to complement automated analysis and detection processes. Manual review is also triggered by incidents, customer requests, escalations, or any other incident impacting production functionality. Security logs are retained in a restricted repository for 400 days to support investigations of security incidents and to meet regulatory retention requirements. Cognite Data Fusion® and underlying infrastructure has all-day support and monitoring. In addition there is a Cognite Engineering on-call rotation for escalation. Cognite uses an automated solution to scramble critical alerts to the on-call engineer outside business hours. On-call engineers are preselected, trained, and assigned roles to perform the required identify, contain, and restore operations. Additional resources, either internally or by cloud service providers, are engaged by the on-call engineer when needed. The process is regularly tested (including tabletop and simulations) to ensure efficacy. The process is part of the Cognite Management System.

Want to know more about our product?

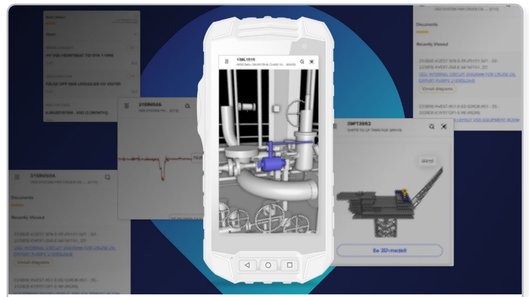
Explore more insights from Cognite



PRODUCT TOUR

Learn from Cognite customers and product managers how Cognite Data Fusion® simplifies and streamlines the data experience of a subject matter expert.

WATCH NOW →



CUSTOMER STORIES

Discover how Cognite Data Fusion® makes data more accessible and meaningful, driving insights that unlock opportunities in real-time, reduce costs, and improve the integrity and sustainability of your operations.

GO TO STORIES →

ANALYST REPORT

Customer interviews and financial analysis reveal an ROI of 400% and total benefits of $21.56M over three years for the Cognite Data Fusion® platform.

READ THE REPORT →

BLOG

Discover our rich catalog of industry insights and technology deep dives.

READ OUR NEWEST BLOGS →

WHY COGNITE DATA FUSION® → BENEFITS FOR YOUR TEAMS → CONTACT SALES →

COGNITE

COGNITE.COM →