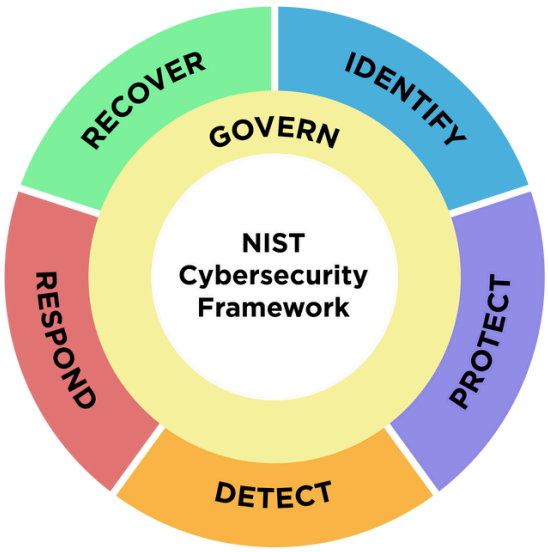
Confidencial

NIST Cybersecurity Framework 2.0



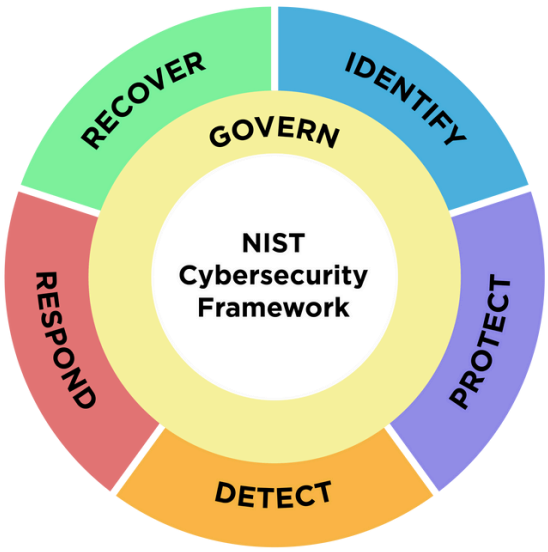
Function: Identify (ID)

Confidencial aligns with the **Identify** category by helping organizations systematically detect and manage sensitive data risks. Below are key ways in which Confidencial supports identification.

CATEGORY	CAPABILITIES
Asset Management (ID.AM)	• Automatically scans cloud and on-prem environments to discover unstructured sensitive data (e.g., contracts, financial records, IP). • Maps where sensitive data resides, who has access to it, and how it's being shared.
Risk Assessment (ID.RA)	• Identifies high-risk unprotected data across storage locations. • Integrates threat intelligence (ID.RA-02) to assess external and internal risks.
Cybersecurity Supply Chain Risk Management (GV.SC)	• Enables secure data sharing with third parties to reduce supply chain risks. • Monitors vendor access and enforces third-party compliance requirements.

Confidencial

NIST Cybersecurity Framework 2.0



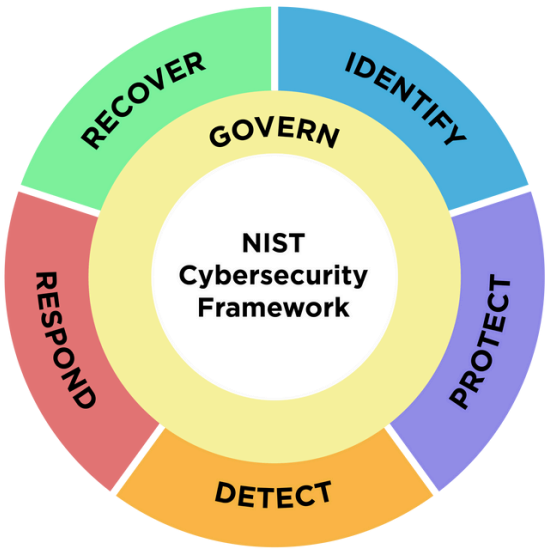
Function: Detect (DE)

Confidencial aligns with the **Detect** category through continuous monitoring, automated threat detection, and real-time visibility into data sharing. This proactive approach helps organizations quickly identify anomalies and secure critical assets. Below are key ways in which Confidencial supports detection.

CATEGORY	CAPABILITIES
Anomalous Activity Detection (DE.AE & DE.CM)	• Flags unexpected data access or sharing behaviors that may indicate insider threats or credential compromise. • Detects when sensitive files are being accessed, copied, or shared in unusual ways.
Security Continuous Monitoring (DE.CM)	• Provides real-time visibility into where unprotected sensitive data exists across the organization. • Monitors data movement to detect unauthorized access attempts.
Threat Intelligence & Monitoring (DE.AE-07 & ID.RA-02)	• Identifies potential data exposure risks by integrating cyber threat intelligence feeds (ID.RA-02). • Supports integration with SIEM/SOAR tools to correlate data risks with broader security threats (DE.AE-07).

Confidencial

NIST Cybersecurity Framework 2.0



Function: Protect (PR)

Confidencial aligns with the **Protect** category through identity management, authentication, access control, data security, and platform security. These capabilities allow organizations to track sensitive data throughout its lifecycle, identify vulnerabilities, and monitor access. Below are key ways in which Confidencial supports protection.

CATEGORY	CAPABILITIES
Identity Management, Authentication, and Access Control (PR.AA)	• Implements granular access controls to enforce least-privilege access to sensitive information. • Provides persistent protection that follows sensitive data, even when data is shared or moved. • Enables organizations to define, manage and enforce data access policies across connected storage environments.
Data Security (PR.DS)	• Secures sensitive data across multiple document types. • Automatically identifies sensitive data types. • Monitors and controls how sensitive information is shared to prevent unauthorized exposure. • Provides detailed mapping of where sensitive data resides, throughout its lifecycle.
Platform Security (PR.PS)	• Enables standardized security configurations across connected storage environments. • Generates comprehensive logs of data access, usage, and sharing activities. • Provides continuous evaluation of security configurations and data protection measures to identify potential vulnerabilities.