



Mapping the Lepide Data
Security Platform to
**NIST Cybersecurity
Framework (CSF)**

Key Activity	Control Text	Technology Alignment
Access Control	<p>ID.AM-4: External information systems are catalogued.</p> <p>ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value.</p> <p>PR.AC-1: Identities and credentials are managed for authorized devices and users</p> <p>PR.AC-3: Remote access is managed</p> <p>PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties</p> <p>PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)</p> <p>PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality</p>	<p>Lepide Identify (Data Discovery and Classification)</p> <p>Lepide Trust (Access Governance)</p> <p>Lepide Insight (User and Entity Behavioural Analytics)</p>
Logging, Monitoring and Alerting	<p>PR.DS-4: Adequate capacity to ensure availability is maintained</p> <p>PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy</p> <p>DE.CM-1: The network is monitored to detect potential cybersecurity events</p> <p>DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events</p> <p>DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events</p> <p>DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed</p> <p>DE.DP-2: Detection activities comply with all applicable requirements</p> <p>DE.DP-4: Event detection information is communicated to appropriate parties</p>	<p>Lepide Insight (User and Entity Behavioural Analytics)</p> <p>Lepide Detect (Threat Detection and Response)</p>

Key Activity	HIPAA Specific Control Area	Technology Alignment
Logging, Monitoring and Alerting (continued)	<p>DE.DP-5: Detection processes are continuously improved</p> <p>RS.AN-1: Notifications from detection systems are investigated</p>	<p>Lepide Insight (User and Entity Behavioural Analytics)</p> <p>Lepide Detect (Threat Detection and Response)</p>
Systems Security	<p>PR.DS-5: Protections against data leaks are implemented</p> <p>PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained</p> <p>PR.IP-3: Configuration change control processes are in place</p> <p>PR.PT-4: Communications and control networks are protected</p> <p>DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed</p>	<p>Lepide Insight (User and Entity Behavioural Analytics)</p> <p>Lepide Detect (Threat Detection and Response)</p>
Incident Response	<p>PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed</p> <p>DE.AE-2: Detected events are analyzed to understand attack targets and methods</p> <p>DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors</p> <p>DE.AE-4: Impact of events is determined</p> <p>DE.AE-5: Incident alert thresholds are established</p> <p>RS.RP-1: Response plan is executed during or after an event</p> <p>RS.CO-2: Events are reported consistent with established criteria</p> <p>RS.CO-3: Information is shared consistent with response plans</p> <p>RS.AN-2: The impact of the incident is understood</p>	<p>Lepide Insight (User and Entity Behavioural Analytics)</p> <p>Lepide Detect (Threat Detection and Response)</p>

Key Activity	HIPAA Specific Control Area	Technology Alignment
Incident Response (continued)	<p>RS.AN-3: Forensics are performed</p> <p>RS.AN-4: Incidents are categorized consistent with response plans</p> <p>RS.MI-1: Incidents are contained</p> <p>RS.MI-2: Incidents are mitigated</p> <p>RS.IM-1: Response plans incorporate lessons learned</p> <p>RS.IM-2: Response strategies are updated</p> <p>RC.RP-1: Recovery plan is executed during or after an event</p> <p>RC.IM-1: Recovery plans incorporate lessons learned</p> <p>RC.IM-2: Recovery strategies are updated</p> <p>RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams</p>	<p>Lepide Insight (User and Entity Behavioural Analytics)</p> <p>Lepide Detect (Threat Detection and Response)</p>
Risk Analysis and Management	<p>ID.RA-1: Asset vulnerabilities are identified and documented</p> <p>ID.RA-3: Threats, both internal and external, are identified and documented</p> <p>ID.RA-4: Potential business impacts and likelihoods are identified</p> <p>ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk</p> <p>PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties</p> <p>PR.IP-12: A vulnerability management plan is developed and implemented</p> <p>RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks</p>	<p>Lepide Identify (Data Discovery and Classification)</p> <p>Lepide Trust (Access Governance)</p> <p>Lepide Insight (User and Entity Behavioural Analytics)</p> <p>Lepide Detect (Threat Detection and Response)</p>

Lepide Data Security Platform

Core Capabilities

Lepide Identify

(Data Discovery and Classification)

- Discover and classify data in real-time.
- Tag data.
- Data valuation.
- Identify data most at risk.

Lepide Trust

(Access Governance)

- Analyse permissions.
- Identify over privileged employees (least privilege).
- View historic permissions.
- Change permissions.

Lepide Insight

(User and Entity Behavior Analytics)

- View interactions with data.
- View interactions with systems governing access to data.
- Employee audit logs.
- Investigate incidents and breach scenarios.

Lepide Detect

(Threat Detection and Response)

- Detect threats in real-time.
- Baseline/profile employee behaviour.
- Identify anomalous employee behaviour.
- Alert and respond to threats in real-time.



Start a free trial



Get a demo



Get a free risk
assessment