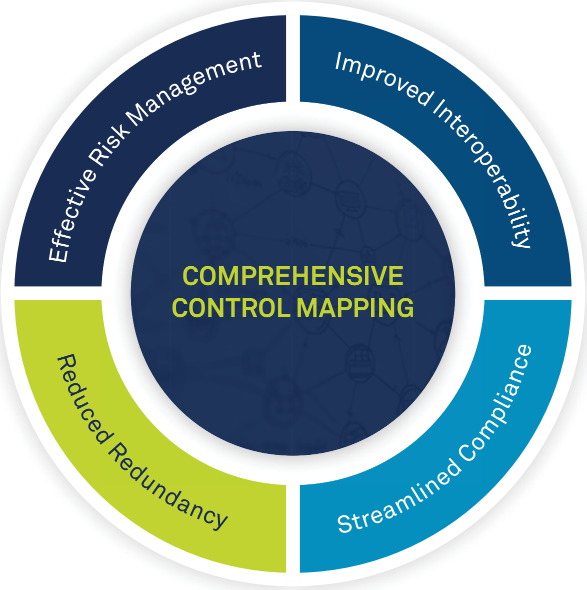
Enhancing Security Posture Through Comprehensive Control Mapping

Comprehensive control mapping demonstrates our commitment to enhanced security assurance, compliance, and transparency while supporting risk reduction and informed decision-making.

Building a Layered Defense

Security control mapping correlates and aligns security controls from various frameworks, standards, or regulations. It is vital for building a robust security posture, ensuring comprehensive coverage, streamlining compliance, enabling effective risk management, reducing redundancy, and facilitating interoperability. The foundational framework for this process is the National Institute of Standards and Technology (NIST), known for its comprehensiveness, risk-based approach, flexibility, and wide recognition. Its role in security control mapping instills confidence, as its coverage includes various standards addressing diverse industries and regulatory requirements globally.


Effective Risk Management
Improved Interoperability
COMPREHENSIVE CONTROL MAPPING
Reduced Redundancy
Streamlined Compliance

Proactive Risk Mitigation

Optimized Resource Allocation

Demonstrated Due Diligence

Adaptability to Change

Comprehensive Control Mapping

1

What is security control mapping?
Security control mapping correlates and aligns security controls from various frameworks, standards, or regulations. Identifying similarities and gaps between security requirements helps organizations streamline compliance efforts, avoid redundant controls, and ensure comprehensive security coverage.

3

Robust Cybersecurity and Privacy
NIST SP 800-53 Rev. 5 is a globally recognized, comprehensive cybersecurity framework. Its strengths lie in its detailed controls, risk-based approach, flexibility, and government backing, making it a top choice for organizations seeking robust cybersecurity and compliance.

5

Medidata's Commitment to Customer Trust
The framework coverage ensures that Medidata maintains a robust security posture across diverse organizations and industries, emphasizing data protection, compliance, and risk management. At the heart of our commitment to customers is trust. Our security control mapping demonstrates the security frameworks necessary to exhibit confidence in our data protection and security practices. By emphasizing data protection, compliance and risk management, we help customers avert threats and safeguard their data.

2

Why is it important?
Security control mapping is crucial for establishing a solid security posture. It provides comprehensive coverage, simplifies compliance, enhances risk management, minimizes redundancy, and improves interoperability. This enables organizations to protect their assets effectively, meet regulatory requirements, and streamline security efforts.

4

Framework Coverage?
The security control mapping encompasses a comprehensive set of frameworks catering to various sectors and regions. It includes NIST SP 800-53 for US federal systems, FedRAMP Moderate for cloud service providers handling US federal data, ISO 27001/2:2022 for establishing and improving information security management systems, SOC2 Type 2 for assessing controls in service organizations, C5 for cloud service providers in Germany, ISMAP for managing information system security, CMMC for defense contractors handling CUI, UK Cloud Act for CSPs in the UK, ANSSI SecNumCloud 3.2 for CSPs in France, and ACN for Italian cybersecurity practices.

For a more in-depth discussion, please contact the Medidata Security Governance team at

MedidataGlobalSecurityGovernance@3ds.com

Medidata, a Dassault Systèmes company, is leading the digital transformation of life sciences.
Discover more at **www.medidata.com** and follow us **@medidata**. Contact us at **info@medidata.com** | **+1 866 515 6044**