Altius IT Policy Collection
Compliance and Standards Matrix Overview

Standards
All organizations, regardless of size, need to secure their data and intellectual property. Information systems must be protected against unauthorized information disclosure (confidentiality), disruption (availability), and reliability (integrity).

Standards represent the knowledge of a large number of experts and provide security implementation recommendations. Each standard helps an organization address security related issues.

- *Control Objectives for Information and Technology (COBIT)* - COBIT is a framework created by the Information Systems Audit and Control Association (ISACA) for information technology governance and management. COBIT is a strategic management tool developed with the help of world-wide experts in the field of IT governance, IT management, performance management, and information security and control. The Altius IT Policy Collection helps organizations meet COBIT information security and control requirements.
- *General Data Protection Regulation (GDPR).* Privacy and security requirements governing the collection, use, or disclosure of a data subject's personal data.
- *International Standards Organization (ISO).* The International Organization for Standardization (ISO) is the world's largest developer and publisher of International Standards. ISO's globally accepted security standards ISO 27001 and 27002 are the de facto standards for information security. In addition to ISO, the protection of personal data is governed by Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), GDPR, and the United Kingdom's Data Protection Act of 1998.
- *National Institute of Science and Technology (NIST)* - NIST develops and issues standards guidelines and other publications to assist organizations in implementing the Federal Information Security Management Act (FISMA) of 2002, the 2014 Framework for Improving Critical Infrastructure Cybersecurity (CSF Cybersecurity Framework), and cost effective programs to protect information and information systems. Federal agencies determine the security category of their information system in accordance with the provisions of Federal Information and Information Systems Standards (FIPS) 199 and then apply the appropriate set of baseline security controls in NIST Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations. Federal Register Vol. 79, No. 222 Minimum Security Controls specifies minimum required security controls for unclassified controlled technical information requiring safeguarding. A description of the security controls is listed in National Institute of Standards and Technology Special Publication 53 (NIST SP 800–53), ‘‘Security and Privacy Controls for Information Systems and Organizations”. A

separate policy addresses NIST SP 800-171 Protecting Controlled Unclassified Information (CUI) requirements.

- *Health (HIPAA, CFR, HITECH, Canada Personal Health Information Protection Act PHIPA)* - Privacy and security rules provide guidelines for safeguarding the use and disclosure of certain confidential medical information known as Protected Health Information (PHI). Specifies data breach disclosure requirements.
- *Payment Card Industry Data Security Standard (PCI DSS)* - PCI DSS helps prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations that store, process, or exchange cardholder information.

References

Each policy and procedure within the collection includes a References matrix that documents the relevant compliance/security reference sources. Version numbers are identified below:

- COBIT - Control Objectives for Information and Related Technologies (2019)
- GDPR - General Data Protection Regulation (2016)
- HIPAA - Health Insurance Portability and Accountability Act (1996) and Health Information Technology for Economic and Clinical Health Act (HITECH) (2009)
- ISO 27001 - International Organization for Standardization Information technology, Security techniques, Information security management systems, Requirements (2022)
- NIST SP 800-37 - National Institute of Standards and Technology (NIST) Special Publication (SP) 37 Risk Management Framework for Information Systems and Organizations (Revision 2)
- NIST SP 800-53 - National Institute of Standards and Technology (NIST) Special Publication (SP) 53 Security and Privacy Controls for Information Systems and Organizations (Revision 5)
- NIST Cybersecurity Framework - National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)
- PCI - Payment Card Industry (PCI) Data Security Standard (Version 4.0)

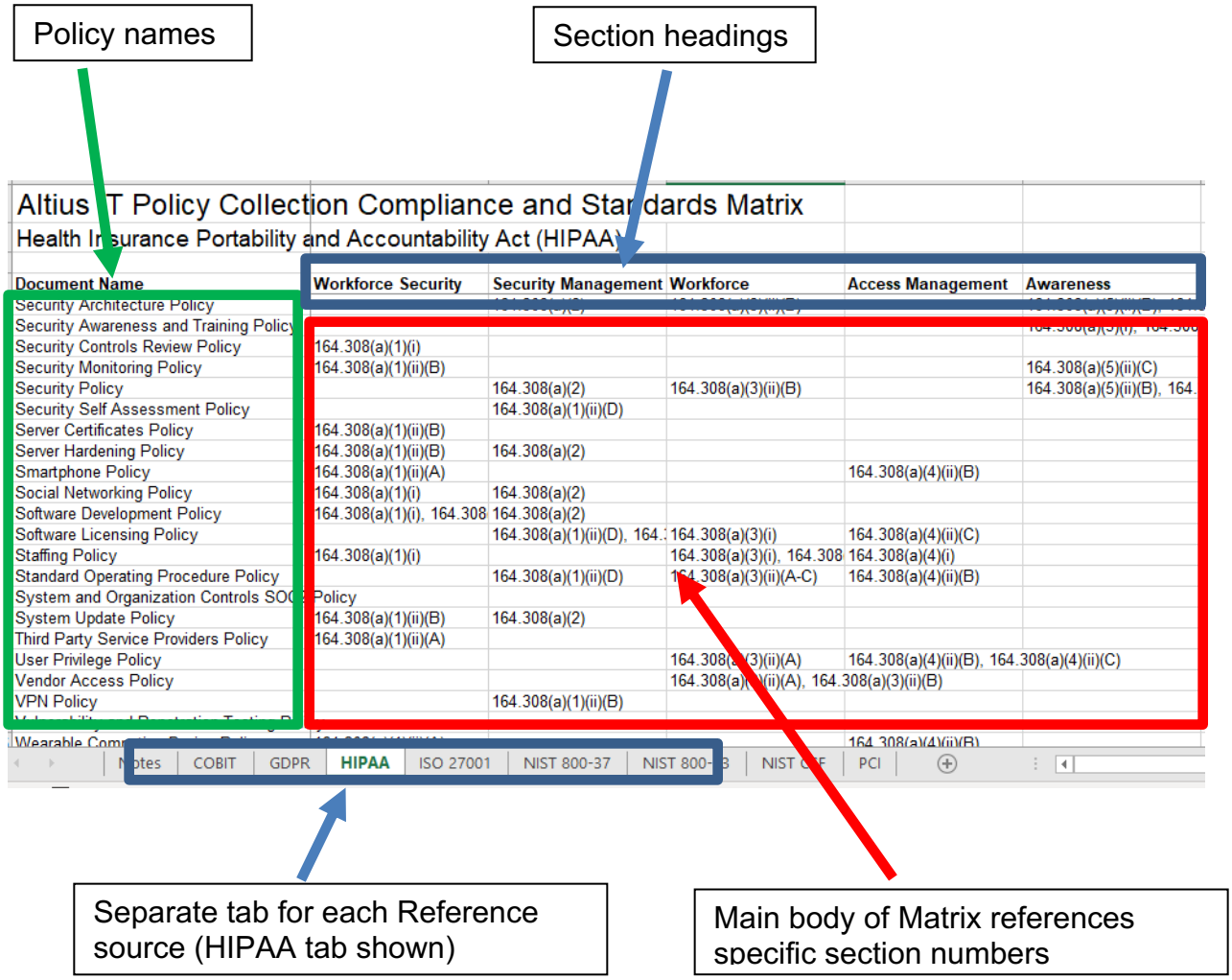
Compliance and Standards Matrix (Excel Spreadsheet)

The Altius IT Policy Collection (www.AltiusIT.com/policies.htm) includes an Excel spreadsheet that provides a cross reference of document names with the relevant compliance/security reference sources for each of the References listed above.

See the following page for an example of the content provided in the Excel spreadsheet.

Altius IT Policy Collection
Compliance and Standards Matrix Overview

Compliance and Standards Matrix – Excel spreadsheet example
Start by selecting the desired Reference tab (e.g. COBIT, GDPR, HIPAA, ISO, NIST, PCI). Detailed information will appear and can be sorted by policy name and/or Reference section number.



Altius IT Policy Collection Compliance and Standards Matrix

Health Insurance Portability and Accountability Act (HIPAA)

Document Name	Workforce Security	Security Management	Workforce	Access Management	Awareness
Security Architecture Policy					
Security Awareness and Training Policy					
Security Controls Review Policy	164.308(a)(1)(i)				
Security Monitoring Policy	164.308(a)(1)(ii)(B)				164.308(a)(5)(ii)(C)
Security Policy		164.308(a)(2)	164.308(a)(3)(ii)(B)		164.308(a)(5)(ii)(B), 164.
Security Self Assessment Policy		164.308(a)(1)(ii)(D)			
Server Certificates Policy	164.308(a)(1)(ii)(B)				
Server Hardening Policy	164.308(a)(1)(ii)(B)	164.308(a)(2)			
Smartphone Policy	164.308(a)(1)(ii)(A)			164.308(a)(4)(ii)(B)	
Social Networking Policy	164.308(a)(1)(i)	164.308(a)(2)			
Software Development Policy	164.308(a)(1)(i), 164.308	164.308(a)(2)			
Software Licensing Policy		164.308(a)(1)(ii)(D), 164.	164.308(a)(3)(i)	164.308(a)(4)(ii)(C)	
Staffing Policy	164.308(a)(1)(i)		164.308(a)(3)(i), 164.308	164.308(a)(4)(i)	
Standard Operating Procedure Policy		164.308(a)(1)(ii)(D)	164.308(a)(3)(ii)(A-C)	164.308(a)(4)(ii)(B)	
System and Organization Controls SOC 2 Policy					
System Update Policy	164.308(a)(1)(ii)(B)	164.308(a)(2)			
Third Party Service Providers Policy	164.308(a)(1)(ii)(A)				
User Privilege Policy			164.308(a)(3)(ii)(A)	164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C)	
Vendor Access Policy			164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B)		
VPN Policy		164.308(a)(1)(ii)(B)			

Notes | COBIT | GDPR | HIPAA | ISO 27001 | NIST 800-37 | NIST 800-53 | NIST CSF | PCI