SHARED ASSESSMENTS

TRUST

USER REFERENCES ON GLOBAL REGULATIONS, STANDARDS AND GUIDELINES MAPPED TO THE SHARED ASSESSMENTS PRODUCTS

Shared Assessments' Third-Party Risk Management (TPRM) Product Suite incorporates a wide body of international laws, regulations, and industry sector guidelines and frameworks in the Standardized Information Gathering (SIG) Questionnaire and the Standardized Control Assessment (SCA) Procedure.

The 2024 SIG contains direct mappings to 27 of the most critical Reference Documents, which are included within the SIG Content Library, as well as the 2024 SCA.

This document lists both the direct mappings in the 2024 SIG and additional mapping "crosswalks" that are available to Shared Assessments Members.

NOTE: Crosswalk Documents show the relationships between content in the regulation, standard, or guideline to the SIG. The matches and gaps between documents, listed in the crosswalk, can help users understand if additional content is needed for their individual compliance needs. Crosswalks may be narrowed to the risk domains found in the Shared Assessments Tools, therefore each user should consult counsel on a case-by-case basis to ensure compliance with all applicable information security and privacy laws, regulations, standards, and guidelines.

2024 SIG DIRECT MAPPING REFERENCES

Industry Standards, Regulations, Guidance			
Mapping Reference	**Asia-Pacific**	**Europe**	**U.S.**
NEW Shared Assessments Standardized Control Assessment (SCA) Procedures, 2024	✓	✓	✓
International Standards Organization (ISO) 27001 and 27002:2022	✓	✓	✓
ISO/IEC 27701: Privacy Information Management Systems (PIMS), 2019	✓	✓	✓
NEW National Institute of Standards and Technology (NIST) Artificial Intelligence 100-1, 2023			✓
NEW National Institute of Standards and Technology (NIST) SP-800-161r1, 2022			✓
NEW NIST SP 800-53 Rev.5 : Security and Privacy Controls for Information Systems and Organizations, 2020			✓
National Institute of Standards and Technology (NIST) Cybersecurity Framework, 2018			✓
NIST Privacy Framework: A Tool for Improving Privacy Through Enteprise Risk Management, 2020			✓
NEW Cybersecurity Maturity Model Certification (CMMC) 2.0, 2021			✓
Center For Internet Security (CIS) Critical Security Controls v8, 2021			✓

2024 SIG DIRECT MAPPING REFERENCES

Industry Standards, Regulations, Guidance			
Mapping Reference	**Asia-Pacific**	**Europe**	**U.S.**
European Banking Authority (EBA) Guidelines on Outsourcing Arrangements, 2019		✔	
European Union (EU) General Data Protection Regulation (GDPR) 2016/679, 2018		✔	
Federal Financial Institutions Examination Council (FFIEC) Architecture, Infrastructure, and Operations (AIO), 2021			✔
FFIEC Outsourcing Technology Services, 2004			✔
North American Electric Reliability Corporation (NERC) Supply Chain Risk Mitigation, 2020			✔
Federal Risk and Authorization Management Program (FedRamp), 2021			✔
NEW Interagency Guidance on Third-Party Relationships: Risk Management 2023			✔
FFIEC Cybersecurity Assessment Tool (CAT), 2017			✔
Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook: Business Continuity, 2019			✔
FFIEC IT Examination Handbook: Management, 2015			✔
NEW SEC Cybersecurity Rule 206(4)-9			✔

2024 SIG DIRECT MAPPING REFERENCES

Industry Standards, Regulations, Guidance			
Mapping Reference	**Asia-Pacific**	**Europe**	**U.S.**
New York Department of Financial Services (NYDFS) Cybersecurity Requirements for Financial Services Companies 23 NYCARR 500, 2017			✓
U.S. Department of Health and Human Services (HHS): Health Information Portability and Accountability Act (HIPAA) Administrative Simplification, 2013			✓
CSA Consensus Assessments Initiative Questionnaire (CAIQ) v4, 2021	✓	✓	✓
Cloud Security Alliance (CSA) Cloud Control Matrix v4.0.1, 2021	✓	✓	✓
International Society of Automation (ISA) 62443-4-1: Secure Product Development Lifecycle, 2018	✓	✓	✓
ISA 62443-4-2: Technical Security Requirements for Identification and Authentication Control Systems, 2018	✓	✓	✓
Payment Card Industry Data Security Standard: Requirements and Testing Procedures (PCI DSS) 4.0, 2022	✓	✓	✓

2023 SIG CROSSWALK REFERENCES
SECURE CONTROLS FRAMEWORK (SCF)

The SCF is a global metaframework comprised of cybersecurity and privacy-related policies, standards, procedures, and prominent frameworks that address nearly all applicable statutory, regulatory and contractual requirements an organization may encounter.

Using the SCF, risk control questions in the SIG 2024 map to and from hundreds of unique national and international frameworks, laws and regulations. The SCF significantly expands the universe of authoritative references available to custom scope a SIG, or to scope a SIG Questionnaire from an authoritative reference not included in the SIG direct mappings.

Notable SCF national sources

NIST 800-171A and NIST 900-171 r2
OWASP Top 10 v2017
US Cert RMM v1.2
US DOD US CMMC 2.0 v1.02
US DOJ/FBI Cert RMM v1.2,
US FDA 21 CFR Part 11
US IRS Publication 1075

Notable SCF international sources

EMEA EU e-Privacy and GDPR
EMEA Personal Data Act: Finland
EMEA France – 78.17/2004 8021
Hong Kong Personal Data Ordinance
People's Republic of China Personal Information Protection Law

REFERENCE DOCUMENTS
HISTORIC SIG REFERENCES

Industry Standards, Regulations, Guidance			
Mapping Reference	**Asia-Pacific**	**Europe**	**U.S.**
EBA Guidelines on Information and Communication Technology (ICT) and Security Risk Management, 2019		✔	
EU/APEC (Asia-Pacific Economic Cooperation) Referential on Personal Data Protection and Privacy Requirements of Binding Corporate Rules (BCR) and Cross-Border Privacy Rules (CBPR), 2014		✔	
EU Parliament/Council of the EU Directive on Security of Network and Information Systems (NISD), 2016		✔	
EU Payment Services Directive (PSD2) 2015/2366, 2018		✔	
National Bank of Belgium (NBB) Outsourcing Regulatory Framework (7.1-7.5), 2019		✔	
United Kingdom (UK) Centre for the Protection of National Infrastructure-Security for Industrial Control Systems: Manage 3rd Party Risk, A Good Practice Guide (CPNI SICS), 2015		✔	

REFERENCE DOCUMENTS
HISTORIC SIG REFERENCES

Industry Standards, Regulations, Guidance			
Mapping Reference	**Asia-Pacific**	**Europe**	**U.S.**
UK Financial Conduct Authority Systems & Controls (FCA-SYSC 8.1): General Outsourcing Requirements, 2018		✓	
UK National Cyber Security Centre - Cyber Essentials, 2015		✓	
UK Ministry of Justice, The Bribery Act 2010 Guidance		✓	
NEW German Supply Chain Act, 2023		✓	
NIST SP 800-184: Guidance for Cybersecurity Event Recovery, 2016			✓
US Office of the Superintendent of Financial Institutions (OFSI) Guideline B-10: Outsourcing of Business Activities, Functions, and Processes, 2009			✓
U.S. Dept of HHS HIPAA: OCR Audit Protocol, 2013			✓
U.S. Department of Defense (DOD) Cybersecurity Maturity Model Certification (CMMC v1.0), 2020			✓
U.S. Department of Defense (DOD) Cybersecurity Maturity Model Certification (CMMC) v1.0, 2020			✓

REFERENCE DOCUMENTS
HISTORIC SIG REFERENCES

Industry Standards, Regulations, Guidance			
Mapping Reference	**Asia-Pacific**	**Europe**	**U.S.**
NEW New York Department of Financial Services (NYDFS) Climate Guidance, 2021			✔
U.S. Office of the Comptroller (OCC) Bulletin 2103-29-Third Party Relationships, 2013			✔
Asia-Pacific Economic Cooperation (APEC) Referential on Personal Data Protection and Privacy Requirements of Binding Corporate Rules (BCR) and Cross Border Privacy Rules (CBPR), 2014	✔		
Australian Prudential Regulatory Authority, (APRA) Prudential Protection Guide CPG 234-Management of Security Risk in Information and Information Technology, 2017	✔		
Australian Government Department of Defense (AU DOD) Essential 8	✔		
Hong Kong Monetary Authority (HKMA), SA-2-Outsourcing, 2001	✔		
HKMA: TM-G-1 General Principles for Technology Risk Management, 2003	✔		
Monetary Authority of Singapore (MAS) Technology Risk Management Guidelines (TRMG), 2013	✔		