USER REFERENCES ON REGULATIONS, STANDARDS AND GUIDELINES MAPPED TO SHARED ASSESSMENTS PROGRAM TOOLS

Shared Assessments keeps a close eye on emerging risks, regulations, guidelines and standards for the wide range of industries that our members represent.

Accordingly, the components of the Shared Assessments Third Party Risk Toolkit take into account a wide body of international regulatory requirements and industry standards, including those referenced in this document.

Reference Documents have been mapped to the Standardized Information Gathering (SIG) questionnaire, which aligns to the Standardized Control Assessment (SCA) procedures.

This mapping is available exclusively to Shared Assessments Members upon request. Crosswalk Documents show the relationships between content in the regulation, standard or guideline to the SIG and SCA. 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.

The 2022 SIG contains direct mappings to eighteen of the most critical Reference Documents included within the SIG Content Library, as well as the content from the SCA. Those eighteen mappings to Reference Documents are included within the body of the SIG and can therefore be used for creating custom questionnaires and quickly referenced without accessing additional documents.

SHARED ASSESSMENTS REFERENCE DOCUMENTS

Asia-Pacific Industry Standards, Regulations and Guidance:	Mapped To SIG	Mapping In The 2022 SIG
Asia-Pacific Economic Cooperation (APEC) Referential on Personal Data Protection and Privacy Requirements of Binding Corporate Rules (BCR) and Cross Border Privacy Rules (CBPR), Feb 2014	X	
Australian Prudential Regulatory Authority (APRA) Prudential Practice Guide CPG 234-Management of Security Risk in Information and Information Technology, Jan 2017	X	
Australian Govt Dept of Defense (AU DOD) Essential 8	X	
Hong Kong Monetary Authority (HKMA): SA-2-Outsourcing, Dec 2001	X	
HKMA: TM-G-1 General Principles for Technology Risk Management, 2003	X	
Monetary Authority of Singapore (MAS) Technology Risk Management Guidelines (TRMG) 2013	X	

International Industry Standards, Regulations and Guidance:	Mapped To SIG	Mapping In The 2022 SIG
Cloud Security Alliance (CSA) Cloud Controls Matric (CCM) v.4.0.1, 2021	X	X
CSA Consensus Assessments Initiative Questionnaire (CAIQ) v.4, 2021	X	X
ISA 62443-4-1	X	X
ISA 62443-4-2	X	X
International Standards Organization (ISO) 27001 and 27002:2013	X	X
ISO PIMS, Aug 2019	X	X
PCI DSS 3.2.1, 2018	X	X
Shared Assessments Standardized Control Assessment (SCA) Procedures	X	X

SHARED ASSESSMENTS REFERENCE DOCUMENTS

North American Industry Standards, Regulations and Guidance:	Mapped To SIG	Mapping In The 2022 SIG
Nat'l Institute of Standards and Technology (NIST) Cybersecurity Framework, April 2018	X	X
NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management	X	X
NIST SP 880-53 r5, Security and Privacy Controls for Federal Information Systems and Organizations	X	X
NIST Sp 800-184, Guidance for Cybersecurity Event Recovery, Dec 2016	X	
New York State Dept of Financial Services (NYDFS) Cybersecurity Requirements for Financial Services Companies 23 NYCRR 500	X	X
U.S. Office of the Comptroller (OCC) Bulletin 2103-29-Third Party Relationships, Oct 2013	X	
U.S. Office of the Superintendent of Financial Institutions (OFSI) Guideline B-10: Outsourcing of Business Activities, Functions, and Processes, March 2009	X	
Federal Financial Institutions Examination Council's (FFIEC) IT Examination Handbook: Revised Business Continuity Management Booklet, Nov 2019	X	X
FFIEC Cybersecurity Assessment Tool (CAT) May 2017	X	X
FFIEC IT Examination Handbook: Management, Nov 2015	X	X
U.S. Dept of Health and Human Services (HHS) Health Information Portability and Accountability Act (HIPAA) OCR Audit Protocol, March 2013	X	
HHS HIPAA Administrative Simplification, March 2013	X	X
U.S. Dept of Defense, Cybersecurity Maturity Model Certification (CMMC)	X	

SHARED ASSESSMENTS REFERENCE DOCUMENTS

European Industry Standards, Regulations and Guidance:	Mapped To SIG	Mapping In The 2022 SIG
European Banking Authority (EBA) Guidelines on Outsourcing Arrangements, Feb 2019	X	X
EBA Guidelines on ICT and Security Risk Management	X	
European Union (EU)/APEC Referential on Personal Data Protection and Privacy Requirements of Binding Corporate Rules (BCR) and Cross Border Privacy Rules (CBPR), Feb 2014	X	
EU Parliament/Council of the EU Directive on Security of Network and Information Systems (NISD) July 2016	X	
EU General Data Protection Regulation (GDPR) 2016/679, May 2018	X	X
EU Payment Services Directive (PSD2) 2015/2366, Jan 2018	X	
National Bank of Belgium (NBB) Outsourcing Regulatory Framework (7.1-7.5), July 2019	X	
UK Centre for the Protection of National Infrastructure-Security for Industrial Control Systems, Manage Third Party Risk, A Good Practice Guide (CPNI SICS), May 2015	X	
UK Financial Conduct Authority Systems and Controls (FCA SYSC)-Outsourcing 8.1, March 2018	X	
UK National Cyber Security Centre - Cyber Essentials, Jan 2015	X	
UK Ministery of Justice - The Bribery Act 2010 Guidance	X	