User References on Regulations, Standards and Practices

Shared Assessments keeps a close eye on emerging risks, as well as emerging 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 domestic and international regulatory requirements and industry standards, including those referenced here.

Some Reference Documents have also been mapped to the Standardized Information Gathering (SIG) Questionnaire and the Standardized Control Assessment (SCA). This mapping is available exclusively to Shared Assessments Members upon request. As with the mappings contained within the SIG, Crosswalk Documents show relationships between content in the SIG and SCA. The matches and gaps between documents can help users understand if additional content is needed for their individual compliance needs. Crosswalks may be narrow in scope, and each user should consult counsel on a case-by-case basis to ensure compliance with all applicable information security and privacy laws, regulations, policies and standards.

The 2020 SIG contains direct mappings to ten of the most critical Reference Documents included within the SIG Content Library, as well as the content from the SCA. Those ten mappings to Reference Documents are also included within the body of the SIG and can therefore be used for creating custom questionnaires and quickly referenced without accessing additional documents.

2020 REFERENCE DOCUMENTS	Controls Included In SIG	Content Mapped to SIG	Mapping Included Within SIG
International Industry Standards, Regulations and Guidance:			
Bank for International Settlements (BIS) and International Organization of Securities Commissions (IOSCO) - Guidance on cyber resilience for financial market infrastructures - June 2016	X	X	
Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) V3.0.1, 2014	X	X	
CSA Consensus Assessments Initiative Questionnaire (CAIQ) V3.1	X	X	
International Standards Organization (ISO) 27001/27002, 2013 - **CONTENT UPDATED**!	X	X	X
Payment Card Industry (PCI DSS) V.3.2.1, February 2018 **MAPPING UPDATED!**	X	X	X
Shared Assessments Standardized Control Assessment (SCA) Procedure Tools, November, 2019 **MAPPING UPDATED!**	X	X	X
Asia-Pacific Industry Standards, Regulations and Guidance:			
Australian Prudential Regulatory Authority (APRA) Prudential Practice Guide CPG 234 - Management of Security Risk in Information and Information Technology, May 2013	X	X	
Hong Kong Monetary Authority (HKMA): SA-2-Outsourcing (2001)	X	X	
Hong Kong Monetary Authority (HKMA): TM-G-1-General Principles for Technology Risk Management (2003)	X	X	
Association of Banks in Singapore Outsourced Service Provider (OSP) Standardized Guidelines, June 2015	X	X	
Monetary Authority of Singapore (MAS) - Technology Risk Management Guidelines (TRMG) March 2013	X	X	
European Industry Standards, Regulations and Guidance:			
European Banking Authority (EBA) Guidelines on Outsourcing Arrangements **NEW!**	X	X	
EU/Asia-Pacific Economic Cooperation (APEC), Referential on Personal Data Protection and Privacy Requirements of Binding Corporate Rules (BCR) and Cross Border Privacy Rules (CBPR) February 2014	X	X	
EU General Data Protection Regulation (GDPR), April 2016 (Effective May, 2018) - **CONTENT and MAPPING UPDATED**!	X	X	X
UK Centre for the Protection of National Infrastructure – Security for Industrial Control Systems (CPNI SICS) - Managing Third Party Risk, May 2015	X	X	
UK Financial Conduct Authority Systems and Controls (FCA SYSC) – Outsourcing 8.1, May 2016	X	X	
UK Modern Slavery Act - Transparency in Supply Chain Provisions, October 2015 **NEW!**	X		
UK National Cyber Security Centre - Cyber Essentials, January 2015	X	X	

2020 REFERENCE DOCUMENTS	Controls Included In SIG	Content Mapped to SIG	Mapping Included Within SIG
North American Industry Standards, Regulations and Guidance:			
American Institute of Certified Public Accountants (AICPA) – Template for Breach of Personal Information, 2004	X		
California Consumer Privacy Act (CCPA) (As of September 13, 2018 passage) **NEW!**	X		
Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) **NEW!**	X		
National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) v1.1, April 2018 - **CONTENT AND MAPPING UPDATED**!	X	X	X
NIST Special Publication (SP) 800-53 Revision 4 – Security and Privacy Controls for Federal Information Systems and Organizations, January 2015 - **CONTENT and MAPPING UPDATED**!	X	X	X
NIST SP 800-184_Guidance for Cybersecurity Event Recovery		X	
NIST SP 800-61 Revision 2 – Computer Security Incident Handling Guide, August 2012	X		
NIST SP 800-184, Guidance for Cybersecurity Event Recovery, 2016	X		
New York State Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR 500), 2017 - **CONTENT and MAPPING UPDATED**!	X	X	X
U.S. Department of Treasury, Office of the Comptroller (OCC) Bulletin 2013-29 – Third-Party Relationships, October 2013	X	X	
U.S. OCC Merchant Handbook/Risk Management & Controls/Managing third party organizations August 2014	X		
U.S. Department of Treasury, Office of Foreign Assets Control (OFAC) - A Framework for OFAC Compliance Commitments **NEW!**	X		
U.S. Computer Emergency Readiness Team (CERT) – Federal Incident Notification Guidelines, October 2014	X		
U.S. Cyber Consequences Unit (CCU) Cybersecurity Matrix, 2009	X		
U.S. Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT), May 2017 **MAPPING UPDATED!**	X	X	X
U.S. FFIEC Information Technology Examination Handbook – Appendix J: Strengthening the Resilience of Outsourced Technology Services, February 2015	X	X	X
U.S. FFIEC Information Technology Examination Handbook – Management, February 2015	X	X	
U.S. FFIEC Information Technology Examination Handbook – Information Security, February 2015 **MAPPING UPDATED!**	X	X	X
U.S. Food and Drug Administration (FDA) Title 21 of the Code of Federal Regulations (CFR) Part 11 (Electronic Records) Section 11.1(a), April 2016	X	X	
U.S. Department of Health and Human Services (HHS). Health Insurance Portability and Accountability Act (HIPAA) Final Rule Modifications, March 2013	X		
U.S. Department of Health and Human Services Office of Civil Rights (HHS OCR) Health Information Portability and Accountability Act (HIPAA) Administrative Simplification – March 2013 **MAPPING UPDATED!**	X	X	X