SFG | SHARED ASSESSMENTS
The Trusted Source in Third Party Risk Management

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

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 international regulatory requirements and industry standards, including those referenced on this page.

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 2021 SIG contains direct mappings to fourteen of the most critical Reference Documents included within the SIG Content Library, as well as the content from the SCA. Those fourteen 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.

2021 TOOL RELEASE REFERENCE DOCUMENTS	Mapped to SIG	Mapping listed in the 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	
Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) V3.0.1, 2015	X	
CSA Consensus Assessments Initiative Questionnaire (CAIQ) V3.1	X	
International Society of Automation (ISA) 62443-4-1, Security for industrial automation and control systems Part 4-1: Product security development life-cycle requirements, 2018	X	
International Society of Automation (ISA) 62443-4-2, Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components, 2nd Printing	X	
International Standards Organization (ISO) 27001 and 27002:2013	X	X
International Standards Organization (ISO)/ International Electrotechnical Commission (IEC) 27701 Privacy Information Management System (PIMS) August 2019	X	X
Payment Card Industry (PCI) Data Security Standard (DSS) 3.2.1 May 2018	X	X
Shared Assessments Standardized Control Assessment (SCA) Procedures 2021, September 2020	X	X

Asia-Pacific Industry Standards, Regulations and Guidance:

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	
Association of Banks in Singapore (ABS) Outsourced Service Provider (OSP) Standardized Guidelines, June 2015	X	
Australian Prudential Regulatory Authority (APRA) Prudential Practice Guide CPG 234 - Management of Security Risk in Information and Information Technology, January 2017	X	
Hong Kong Monetary Authority (HKMA): SA-2-Outsourcing, December 2001	X	
Hong Kong Monetary Authority (HKMA): TM-G-1-General Principles for Technology Risk Management (2003)	X	
Association of Banks in Singapore Outsourced Service Provider (OSP) Standardized Guidelines, June 2015	X	
Monetary Authority of Singapore (MAS) - Technology Risk Management Guidelines (TRMG) March 2013	X	

European Industry Standards, Regulations and Guidance:

European Banking Authority (EBA) Guidelines on Outsourcing Arrangements, February 2019	X	
European Banking Authority (EBA) Guidelines on the Security Measures for Operational and Security Risks Under PSD2, January 2018	X	
European Union (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	
European Banking Authority (EBA) Guidelines on Outsourcing Arrangements February 2019	X	X
European Union (EU) Parliament/Council of the European Union Directive on security of network and information systems (NISD) July 2016	X	
European Union (EU) General Data Protection Regulation (GDPR) 2016/679, May 2018	X	X
European Union (EU) Payment Services Directive 2 (PSD 2) - 2015/2366, January 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 Financial Conduct Authority Cyber Resilience Self-Assessment Questionnaire, November 2019	X	
UK Ministry of Justice – Modern Slavery Act - Transparency in Supply Chain Provisions, October 2015	X	
UK National Cyber Security Centre - Cyber Essentials, January 2015	X	
UK Ministry of Justice – The Bribery Act 2010 Guidance	X	

North American Industry Standards, Regulations and Guidance:

National Institute of Standards and Technology (NIST) Cybersecurity Framework April 2018	X	X
National Institute of Standards and Technology (NIST) Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management	X	X
National Institute of Standards and Technology (NIST) SP 800 53 rev. 4 Security and Privacy Controls for Federal Information Systems and Organizations	X	X
National Institute of Standards and Technology (NIST) SP 800-184_Guidance for Cybersecurity Event Recovery, December 2016	X	
New York State Department of Financial Services (NYDFS) Cybersecurity Requirements for Financial Services Companies 23 NYCRR 500	X	X
U.S. Office of the Comptroller (OCC) Bulletin 2013-29 – Third-Party Relationships, October 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 November 2019	X	X
Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity Assessment Tool (CAT) May 2017	X	X
Federal Financial Institutions Examination Council's (FFIEC) IT Examination Handbook: Management November 2015	X	
Federal Financial Institutions Examination Council's (FFIEC) IT Examination Handbook: Revised Business Continuity Management Booklet, November 2019	X	
Federal Financial Institutions Examination Council's (FFIEC) Information Technology Examination Handbook – Information Security, September 2016	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	
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 (HHS) Health Information Portability and Accountability Act (HIPAA) OCR Audit Protocol, March 2013	X	
U.S. Department of Health and Human Services, Office for Civil Rights, Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification March 2013	X	X