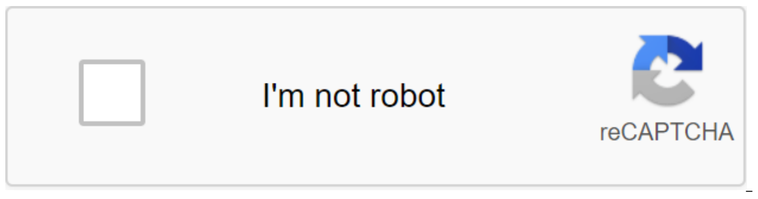
Ffiec manual appendix j



Continue

Page 2 This section is where all the changes made to InfoBase are listed. Each entry of the change includes an effective date and a brief description. Below are the latest InfoBase updates. For a full listing of all the changes, click here: Changing The History of the Magazine November 14, 2019Revised Business Continuity Planning Booklet and a modified name on Business Continuity ManagementThe FFIEC members updated and renamed the Business Continuity Planning Booklet for Business Continuity Management (BCM) to reflect updated information technology risk practices and structures. Members of the Committee developed a brochure using a principle-based approach to IT risk management to ensure that the basic principles of the brochure remained relevant to experts even in the case of innovation and technological change in the financial services sector. Changes included in this brochure include: Changed the name on business continuity management to reflect increased attention to current, corporate continuity and business sustainability. Replaced the term financial institutions with the term entities. Clearer links to NIST, FEMA and other reputable sources. The link between corporate risk management (ERM) and BCM has been clarified. Eliminating the redundant section of pandemic planning. The supply chain risks to individual failure points were discussed. The difference between exercises and tests has been clarified. Increased maintenance and improvement as an important component of the BCM lifecycle. Integrated relevant concepts from the J app to the brochure enclosure. If necessary, agreed definitions and terminology with reputable standards organizations (e.g. NIST and ISO). September 9, 2016 An upcoming brochure on Information Security Updates included removing redundant management materials and refocusing on IT risk management and updating information security processes. This revision reflects changes in the industry, it has streamlined and reordered the concepts of information security throughout the booklet. The updates are consistent with the FFIEC (CAT) CyberSecurity Assessment Tool and the NIST Cybersecurity Framework. The book contains updated examination procedures to help experts assess the adequacy of the institution's culture, management, information security programs, security operations and security processes. April 29, 2016Added Appendix E: Mobile Financial Services for Retail Payment Systems BookletThe update consists of the addition of a new app, Appendix E: Mobile Financial Services. The E app focuses on the risks associated with MFS and emphasizes a corporate approach to risk management to effectively manage and mitigate these risks. The update included: Update the glossary to include terminology in the app. The rest of the brochure remains unchanged. 10 Nov, Nov. Management brochureFul reviewing the management brochure; replaces the June 2004 version. Includes a revised work program. February 6, 2015Ou sustainability of outsourcing technology services Members of FFIEC today released a revised booklet on business continuity planning. The update consists of the addition of a new application entitled Strengthening the Sustainability of Outsourcing Technology Services. The new annex to the Business Continuity Planning Brochure emphasizes that the financial institution's reliance on third-party service providers to perform or support critical operations does not absolve the financial institution of its responsibility to ensure safe and secure operations in external enterprises. An effective third-party management programme should provide a framework for managing financial institutions to identify, measure, monitor and mitigate outsourcing risks. In particular, the financial institution must ensure that its third-party service providers do not adversely affect the ability of the financial institution to properly restore IT systems and return critical functions to normal operation in a timely manner. The application highlights and strengthens the BCP brochure in four specific areas: a third-party cyber resilience testing company on April 2, 2014. April 2, 2014 Statement: Cyberattacks on ATMs and card authorization systems of financial institutions added a joint statement of FFIEC, cyberattacks on ATMs of financial institutions and card authorization systems. This statement identifies the risk associated with current attack vectors against ATM and card authorization systems, and provides mitigation strategies on October 7, 2013. This statement identifies the risk associated with the continued use of the XP operating system. March 22, 2013 Information Technology Examination Handbook InfoBase Improvement Federal Council for Financial Institutions Review (FFIEC) member of agencies today announced the addition of a new feature to the Information Technology Expertise Handbook InfoBase. This feature gives bankers, agency employees, and other stakeholders the ability to register and receive notifications about additions, changes, and deletions from InfoBase. Users can choose to receive either an email notification or real simple syndication (RSS) (RSS) via a link to the online InfoBase page at: ithandbook.ffiec.gov Press Release at: October 31, 2012Uprees of Technology Service Providers (TSP) booklet Replaces the March 2003 version and includes the following changes: Repeals Oversight Policy 1, EDP Interagency Examination, Planning and Distribution Policy, September 1991, and Oversight Policy 11, Advanced Multi-District Data Services Oversight Program (MDPS), January 1995. A programme of risk-monitoring for institutions which outlines the expectations of the agencies regarding the fact that financial institutions have a corporate risk management process that appeals to vendor management for relationships with TSPs. October 31, 2012Referent materials - Administrative guidelines of federal regulators: Implementation of interagency programs to oversee technology service providers Guidelines describe the process of FRS, FDIC and (agencies) to follow the implementation of interagency oversight programs and include the pattern of reporting experts throughout the oversight cycle. The main audience is the leadership of institutions and experts on the ground. July 10, 2012Referent materials Were made public by FFIEC's public statement on cloud computing. In a statement, the cloud computing map risks the various booklets of the FFIEC IT Handbook. May 7, 2012Aunite, BCP, Electronic Banking, Information Security, Operations, Outsourcing, and Retail Payments booklets. Several booklets have been revised to consider the transition from SAS-70 to the SSAE-16 verification process and other third-party verification processes. April 27, 2012 Security Information bookletAdded FFIEC Supplement to Authentication in Internet Banking Environment Guide for All Agencies in The Resource Section, Appendix C. April 9, 2012Outsourcing bookletAdded Appendix D, Managed Security Service Providers (MSSP). This application, including forensic procedures, eliminates the unique risks associated with outsourcing IT security features. Apr 2, 2012The search bookletApras examination procedures to address the risks associated with cloud computing. ON February 23, 2015, the Federal Financial Institutions Examination Board (FFIEC) released an annex to the FFIEC's Business Continuity Planning (BCP) guide to the expertise of FFIEC's Information Technology Review, titled Strengthening the Sustainability of Outsourcing Technology Services. The brochure is part of a series of IT exam guides and provides advice on assisting experts in assessing risk management processes for financial institutions and service providers to ensure the availability of critical financial services. Statement on applicability to institutions with total assets of less than $1 billion: This letter institutions extend to all FDIC-controlled FDIC FDIC Institutions. Highlights: The ANNEX J brochures BCP address the following four key elements of the BCP that the financial institution should consider to ensure that their technology service providers (TSPs) provide sustainable technology services: third-party management. The ability of third parties. Testing with third-party TSPs. Cyber Resilience. An electronic version of the brochure, as well as a FFIEC press release announcing the booklet, are available . OCC Bulletin 2015-9 February 6, 2015 Executive Director of all national banks, federal offices and agencies, Federal Savings Associations; Technology service providers; Heads of departments and departments; All investigative personnel; and other stakeholders the Federal Financial Institutions Review Board (FFIEC) has released a new application strengthening the sustainability of outsourcing technology services to the FFIEC Business Continuity Planning Brochure. The new application ensures that the brochure is consistent with third-party risk management guidelines and includes emerging risks such as cyber resistance risk issues. Business Continuity Planning is one of 11 booklets that include the FFIEC IT Expertise Handbook. This guidance applies to all national banks and federal savings associations (collectively, banks) with external technology services. Community banks should apply risk management practices commensurate with the level of risk and complexity of their external services. The board and management of the community bank must identify the third-party relationships associated with critical technology services and ensure that the bank is always able to manage the risks for risk assessment, monitoring and risk management. Major J Applications emphasizes and strengthens the Business Continuity Planning Booklet in four specific areas: Third party management third-party testing capacity with third-party technology provider Cyber Sustainability Financial Institutions should partner with their technology service provider (s) as needed to enhance the sustainability of outsourcing technologies, as recommended in this guide. Background from October 30, 2013, the Office of the Comptroller of the Currency issued the 2013-29 OCC Bulletin, Third Party Relations: Risk Management Guide. Since many financial institutions depend on third-party providers to support critical banking operations, FFIEC has incorporated these principles, along with other regulatory guidelines, to update the Business Continuity Planning brochure. The updated brochure more effectively addresses the interdependence of third-party services in the overall strategy financial institution's business. As stated in the FFIEC press release, FFIEC IT The handbook is available electronically . For more information, contact Kevin Greenfield, Director of Banking Information Technology, at (202) 649-6340. Bethany Dugan Deputy Comptroller for Operational Risk Link Link