Hewlett Packard Enterprise

Business white paper

Understanding updates and changes to the FFIEC Management Handbook

Increased areas of concern—IT risk management

In November 2015, the Federal Financial Institutions Examination Council (FFIEC) issued an extensively revised and updated version of its management handbook.[1] This may affect your institution, as the new edition expands the governance and risk management sections—especially IT risk management, showing the FFIEC's increased concern in these areas.

Table of contents

Major areas of emphasis in the updated edition:

- Governance—Boards of directors are expected to have a closer role in IT security management.
- Risk management for operational risks—IT managers need to ensure effective IT controls are in place, and departments held accountable.
- IT risk management—Managers must ensure they are measuring and controlling risk exposure in information assets owned by the institution or third parties.

Examination procedures have also been updated, with an added focus on IT governance and IT risk management.

Governance key

The sharpened focus on governance emphasizes the need for the board of directors "to set the tone and direction for an institution's use of IT." Your organization should have an IT strategic plan that includes an IT strategy. The plan must align with your organization's overall business strategy, with the board taking leadership by approving the plan.

The handbook recommends an IT steering committee. With more specific expertise in IT, the committee reports directly to the board on the status and progress of IT initiatives. The steering committee has a charter defining its mission and responsibilities, with the board retaining ultimate responsibility for decisions relating to IT strategy.

IT management roles addressed

The 2015 handbook adds a new heading on IT management, covering the main roles of IT governance. These roles should be in place, or at least someone should be performing the functions of these roles.

Vital roles in IT security management include:

- **Chief Information Officer (CIO)/Chief Technology Officer (CTO)**—Responsible for implementing IT strategy, overseeing IT budget, and accountability for performance of IT staff and assets. The job should be structured so individuals can accomplish their duties with minimal obstacles.
- **Chief Information Security Officer (CISO)**—FFIEC has given this role renewed emphasis. Traditionally responsible for management and mitigation of information security risks, the CISO role has expanded beyond technology to include risk management across the whole enterprise. Management should be structured for the CISO to maintain independence and avoid conflicts of interest.

[1] FFIEC Information Technology Examination Handbook: Management, **http://ithandbook.ffiec.gov/it-booklets/management.aspx**

- **IT line and business unit management**—Duties include coordinating services between data processing and other functions, and reporting to senior management on plans, projects, and performance. Specific activities and roles will vary between institutions, depending on whether the institution uses a centralized or decentralized approach to IT management.

Risk management significant

Risk management is a critical function of your IT operations. Risks must be assessed, understood, and managed across the institution. Of the risks a financial institution faces, the one of primary concern to IT is operational risk. This is the risk resulting from a potential failure in processes, people, or systems. Inadequately managed and controlled IT operations can result in operational risk to an institution.

Operational risks can happen anywhere IT operates, from back office to customer facing. Operational risks in IT can be broken into:

- Strategic risk—Risk resulting from management acting on inaccurate information and making poor strategic decisions.
- Compliance risk—This results from an institution's inability to meet regulatory requirements associated with delivering its products and services.
- Reputational risk—Errors, delays, unauthorized access to IT systems, and loss of customer data can lead to negative public relations impacts to an institution.

Within the risk management function, IT Risk Management (ITRM) supports the institution-wide overall risk management program through four strategies:

- Risk identification—Inventorying systems and information, and identifying threats to systems and operations
- Risk measurement—Qualifying and quantifying risk to the institution
- Risk mitigation—Implementing appropriate controls to reduce risk potential to an acceptable level
- Risk monitoring and reporting—Providing the board and management with updates on the effectiveness of the ITRM program

Risk identification

Risk is always a factor in all IT operations. You cannot make risk management decisions until risks have been identified and understood. Risk identification entails making a full inventory of your institution's information assets, hardware, software, and data. Once this has been done, cybersecurity risks must be identified and analyzed for each asset.

Many factors should be taken into account to understand institutional risks, including a strategic IT plan, information flow, business continuity/disaster recovery plans, audit findings, and others.

Risk measurement

Once you have identified and understand the risks, they must still be measured. Risk measurements can be qualitative, quantitative, or a combination. Subjective surveys and questionnaires are two ways of assessing qualitative risk. Quantitative risk assessments should result in estimating the likelihood of an occurrence and severity of the exploitation's impact based on the identified risk. This may be measured in resources such as time or money lost, litigation or fines, or cost to reputation.

Examples of risks that can have significant impact include security breaches, system failures, external or insider malfeasance, capacity planning, and others.

Do not consider risks only in isolation, as they often have dependencies or interactions with other risks.

Risk mitigation

Once identified and quantified, you can mitigate risks using appropriate controls. There are many methods of risk mitigation, and the approach you choose should be based on the nature of the risk in question.

After controls are implemented, residual risk may remain. Management should determine the level and plan on how to deal with it.

Risk monitoring and reporting

To control IT risk, you have to measure it. Monitoring and reporting IT metrics will help management understand how risk is being managed—if it's increasing or decreasing, or if the nature of the risks is changing.

Risk metrics should be reviewed regularly so that the changing nature of threats is not overlooked.

Focus renewed

The 2015 FFIEC Management Handbook brings a renewed focus on IT governance and risk management. As a financial institution IT leader, you must not only be adept with the technology, but also able to understand risk, while effectively and efficiently governing a complex IT operation.

For support meeting FFIEC guidelines, let Hewlett Packard Enterprise (HPE) Security Strategy and Risk Management consulting practice assist you in building an effective governance and risk management program.

Learn more at
hpe.com/services/security

Sign up for updates

Hewlett Packard Enterprise

4AA6-4028ENW, August 2016, Rev. 1