The Department of Housing and Urban Development
OCIO Risk Management Policy

HUD Handbook 3435.1 Rev. 2

12 March 2019

DOCUMENT CHANGE HISTORY

Issue	Date	Pages Affected	Description
Original	April 19, 2015	All	Initial Version 1.0 Published
Revision	August 2017	All	Draft Version
Revision	August 7, 2018	All	Draft Version
Revision	March 12, 2019	All	Final Version 2.0 Published

TABLE OF CONTENTS

1. Introduction

The Office of the Chief Information Officer (OCIO) Risk Management Policy of the U.S. Department of Housing and Urban Development (HUD) is based on guidance from both the Office of Management and Budget (OMB) and the Government Accountability Office (GAO). This policy guidance includes the management of risks that may affect information technology (IT) assets, including data and information, in agencies to better manage Federal investments in information management and information technologies that support the agency missions.

Risk management involves the process of identifying, assessing, evaluating, and responding to risks for an IT program or project. A principal goal of an organization's risk management process should be to protect not just its IT assets, but also the integrity of the organization and its ability to perform its mission. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT systems, but as an essential IT management function of the entire organization.

The OCIO Risk Management Policy, together with the Information Technology Management (ITM) Framework, integrates Federal mandates, directives, and best practices for managing the risks that may affect IT investments. The ITM Framework focuses on providing transparency, accountability, and responsibility throughout the entire IT management process. Figure 1 shows the components and processes of the ITM Framework, including the Risk Management component within the framework.

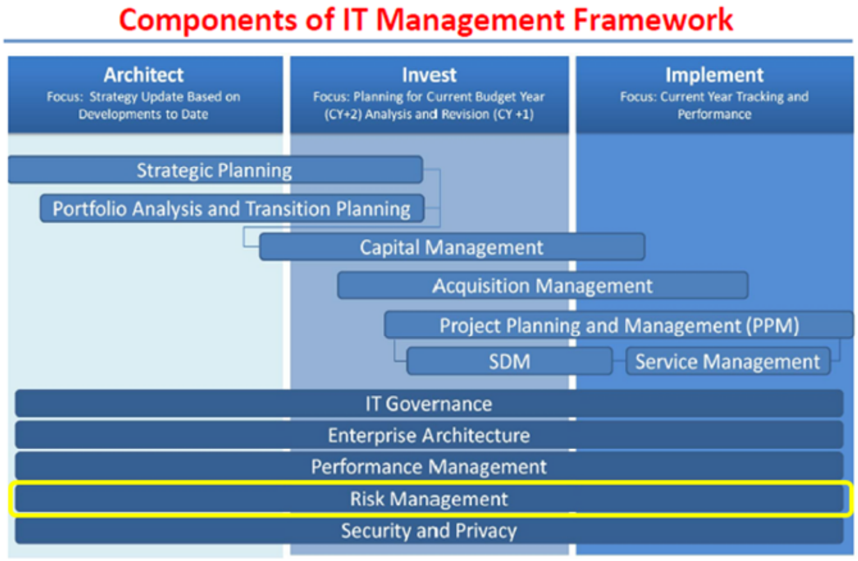
Components of IT Management Framework
Architect
Focus: Strategy Update Based on Developments to Date
Invest
Focus: Planning for Current Budget Year (CY+2) Analysis and Revision (CY +1)
Implement
Focus: Current Year Tracking and Performance
Strategic Planning
Portfolio Analysis and Transition Planning
Capital Management
Acquisition Management
Project Planning and Management (PPM)
SDM
Service Management
IT Governance
Enterprise Architecture
Performance Management
Risk Management
Security and Privacy

Figure 1. Risk Management as a component of the IT Management Framework[1]

[1] HUD Policy for Information Technology Management version 1.0, Handbook No. 3400.1,3. Washington, DC: HUD, April 2011. Retrieved from https://www.hud.gov/sites/documents/34001CIOH.PDF.

Three levels of risk are considered in a thorough risk management approach:

1. enterprise-level risks that threaten the overall IT performance at HUD
2. investment- and program-level risks that threaten the continuity of IT management processes and the ability to implement IT investments
3. project-, system-, and service-level risks that threaten achievement of specific goals or achievement of consistent value from current systems and services.

Proper consideration of risk in investment and project management helps ensure the successful implementation and investment management. Business cases for investment include considerations of performance, cost, and risk to help decision-makers understand and eliminate or reduce factors that could affect successful investment management.

2. Purpose

The OCIO Risk Management Policy provides guidance to ensure that risks[2] associated with HUD's IT investments are effectively identified, considered in decision-making, and managed carefully. There are three major objectives for performing risk management:

- Increase the probability that HUD IT investments will provide HUD stakeholders the expected value from the investment for small to large projects in a safe and secure way.
- Enable management to make risk-informed decisions to justify the expenditures that are part of an IT investment budget.
- Assist management in authorizing (or accrediting) and continuously monitoring and controlling risks that may affect HUD's physical and virtual IT and information systems, environments, and services.[3]

IT investments at HUD are made through, and managed by, the processes and procedures defined in the ITM Framework[4] and the "OCIO Risk Management: Quick Reference

[2] A risk is an uncertain, future condition or event that, if it occurs, can or will affect the objectives of a project negatively or positively. "As commonly defined, a risk can have either a positive or negative effect on a project; that is:

> It can be a threat, which, if it occurs, will endanger the success of a project.

or

> It can be an opportunity which, if acted upon, will enhance the likelihood of project success."

Royer, Paul S. *Project Health Assessment*, 38. Boca Raton, FL: CRC Press, 2015.

[3] For more information about the requirements for managing risks and performance related to virtual IT and information systems, environments, and services (such as cloud computing systems and services), *see* General Services Administration (GSA), *FedRAMP Continuous Monitoring Performance Management Guide version 2.1*. Washington, DC: GSA, February 21, 2018.

[4] Note that this policy addresses the risk management of HUD's IT investments and IT systems. This policy does not deal with other aspects of agency risk management.

Guide to Managing IT Project Risks."[5] As such, IT risk management must be considered together with other ITM Framework policies and guides.

3. Rescission

This version of the handbook represents the updated version of the HUD OCIO Risk Management Policy. The risk management policy published under OCIO-17-13, *HUD Policy for Information Technology Risk Management*, dated August 2017, is rescinded.

4. Applicability

The provisions of this OCIO Risk Management Policy, together with the "OCIO Risk Management: Quick Reference Guide to Managing IT Project Risks," apply to all HUD IT projects and IT systems that store, process, or transmit organizational data and information and to all HUD employees and contractors who use and work with HUD IT investments, portfolios, programs, and projects. Updates to and distribution or transmittal of the HUD OCIO Risk Management Policy are governed by the provisions of the HUD Directives System in Handbook No. 000.2 Rev. 3.

5. Effective Implementation Date

The HUD OCIO Risk Management Policy is already in effect and is awaiting departmental clearance for approved updates. This OCIO Risk Management Policy is applied in conjunction with established Federal statutes, regulations, authorities, guidance, and applicable collective bargaining agreements.

6. Policy

Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. Risks can have a functional impact on business processes or rules, development effort and resources, technology, and capability and management of both physical and virtual information systems, environments, and resources.[6]

Risks can also have positive and negative impacts when considering both the probability and the impact of risks on the project. All HUD IT investments, portfolios, programs, projects and individuals who manage them must consider risk according to the processes and procedures in the ITM Framework, the "OCIO Risk Management: Quick Reference Guide to Managing IT Project Risks," and processes set forth by the HUD Performance and Risk Management Branch (PRMB).

[5] This guide covers the processes for managing risk as it pertains to the HUD IT investment, portfolio, program, or project.

[6] Royer, 13.

This means that:

1. All HUD IT portfolios have identified risks, and managers shall regularly monitor risks and make the necessary adjustments to mitigate the effects on their programs and projects.
2. Selection criteria for capital planning of investments shall include criteria for evaluating risk on IT portfolios.
3. All HUD IT portfolios shall be evaluated by the PRMB to ensure that IT Project Managers (PM) adhere to established standards, guidelines, and procedures for risk management to safeguard agency IT assets, services, and information systems.[7]

As organizations use automated IT systems to process information for better support of their missions in this digital era, risk management plays a critical role in protecting an organization's information assets and, therefore, its mission from IT-related risk. The principal goal of an organization's risk management process is to protect the organization and its ability to perform its mission, in addition to protecting its IT assets.

Considering Risk in Investment Decision-Making

Along with business value and cost, risk is a key consideration in making IT investment funding and management decisions. Decision-makers must be able to evaluate whether the risks involved in a specific situation are acceptable for achieving the expected business value of the IT investment.

As an IT investment progresses, managers must remain alert to changes in identified risks and adjust their actions accordingly. Therefore, HUD risk management is viewed as an active management function, rather than a passive activity. Risks associated with IT investments are weighed by executive decision-makers, along with other agency risks – including financial and external risks in making agency-wide funding decisions.

Decision-making related to risk management also extends to both the ITM Framework and the Project Planning and Management (PPM) version 2.0 that affects the selection, funding, and management of IT investments.

[7] The term "information system" refers to "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." National Institute of Standards and Technology (NIST), *Guide for Conducting Risk Assessments*, NIST Special Publication (SP) 800-30 revision 1, footnote 7. Washington, DC: NIST, September 2012. Retrieved at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. Information systems include general support systems (such as mainframe computers, mid-range computers, local area networks (LAN), and agency-wide backbone systems), in addition to applications that can run on general support systems and whose use of information resources satisfy a specific set of user requirements.

Information Technology Management Framework.[8] The ITM Framework represents a set of policies, procedures, standards, and guidelines that assist HUD's customers in improving mission delivery and in bringing IT into the 21st century to better serve its customers and communities. Risk management is a part of each phase of the ITM Framework, which includes the Architect, Invest, and the Implement phases.

As part of the "Architect" phase of the ITM Framework, IT governance participants scan the environment on an ongoing basis for business risk and business drivers, emerging industry trends, and changing Federal requirements from OMB and other legislative and Executive Office directives. As part of the "Invest" phase of the ITM Framework, IT investments are evaluated against a set of criteria during capital planning that include risk. Assessments of risk during the Invest phase is an important factor in decision-making that affects the selection and funding of IT investments. As part of the "Implement" phase of the ITM Framework, a focus is placed on the subsequent implementation of the project, along with tracking and assessing its performance within the parameters of the approved budget and schedule according to the agreed upon project plans. The Architect, Investment, and Implement components of the ITM Framework work together to reduce or eliminate risk by ensuring that the optimal selection, governance, and performance of IT investments help maintain the alignment of HUD's mission and its strategic goals and objectives.

Project Planning and Management Framework.[9] The PPM 2.0 Framework includes specific procedures, standards, and guidelines for IT investments selected for funding through investment selection criteria for capital management. Each phase of the PPM 2.0 Framework addresses risk and specific requirements. Risk factors are considered decisions to allow a project to pass through a control gate and move to the next phase. Early in the process, the "Planning" phase requires the development of a Risk Management Plan and a risk register or log to lay out the approach for how the project plans to monitor, control, and record risks throughout its life cycle. The performance of the IT portfolio is assessed quarterly by the PRMB. Risk is a significant consideration in these performance evaluations and considered in making portfolio adjustments. The "Invest" phase of the ITM Framework is where projects are managed by following the PPM version 2.0 procedures, standards, and guidelines. The use of Project Risk Management Plans and risk registers or logs started during the Invest stage of the ITM Framework continues from the start of the project through the end of its life cycle.[10]

[8] HUD Policy for Information Technology Management version 1.0, Handbook No. 3400.1, 3. Washington, DC: HUD, April 2011. Retrieved at https://www.hud.gov/sites/documents/34001CIOH.PDF. *See also* IT Management Framework Concept of Operations (CONOPS). Washington, DC: HUD. Retrieved at https://www.hud.gov/program_offices/cio/ITMHOME/Conops.

[9] HUD Policy for Project Planning and Management (PPM) version 2.0. Washington, DC: HUD, October 2015. Retrieved at https://www.hud.gov/sites/documents/34101CIOH.PDF.

[10] Project Planning and Management (PPM) version 2.0 Life Cycle. Washington, DC: HUD, December 17, 2013. Retrieved at https://www.hud.gov/sites/ documents/PPM2CONTROLGATE.PDF.

Risk Management for IT and Information Systems

Risk assessment and risk mitigation, and risk evaluation are key components of the structured risk management approach for IT systems based on guidance in OMB Circular No. A-123,[11] Management's Responsibility for Enterprise Risk Management and Internal Control. This guidance helps agencies modernize existing efforts by requiring them to implement and coordinate Enterprise Risk Management capability with the strategic planning and review processes established by the Government Performance and Results (GPRA) Modernization Act. Internal control processes are also required by the Federal Managers Financial Integrity Act (FMFIA) and the *Green Book* by the GAO.[12] The HUD IT project management life cycle integrates risk management for IT systems throughout the life cycle phases and the approach selected for each specific project during the system development life cycle.[13]

7. Roles and Responsibilities

This section defines the following roles and responsibilities in risk management of IT investments under the HUD OCIO Risk Management Policy.

Office of the Chief Information Officer

The Office of the Chief Information Officer shall:

- Establish an IT risk management framework that incorporates and integrates the various risk management levels and activities (for example, decision-making approach, project management, systems security).
- Provide procedures, standards, and guidelines for IT managers to help them identify, manage (eliminate or reduce), and monitor risk.
- Implement data collection and reporting mechanisms and procedures to assist investment, project, and system managers in collecting, analyzing, and reporting the required risk information.

[11] This Circular is issued under the authority of the Federal Managers Financial Integrity Act of 1982, 31 U.S.C. § 3512, and the Government Performance and Results Modernization Act of 2010, Public Law (Pub. L.) 111-352.

[12] Government Accountability Office, *Standards for Internal Control in the Federal Government* ("*Green Book*"), GAO-14-704G. Washington, DC: GAO, September 2014. Retrieved on April 2, 2018 from https://www.gao.gov/assets/670/665712.pdf.

[13] Note that HUD maintains a separation, although with inevitable overlaps, between the project management life cycle approach and the specific solution develop approach adopted on any project. The project management life cycle provides consistent expectations in terms of personnel management, communications, cost and schedule management, and so on. Each specific development approach – waterfall, Agile, etc. – describes the specific activities and expectations for its successful use. Each of these levels of management has its own risks.

- Work with other agency units (including the Office of Strategic Planning and Management (OSPM) and mission areas within the Office of the Chief Financial Officer (OCFO)) in a coordinated effort to help eliminate or reduce agency-related risks related to financial management and mission delivery.

Technical Review Sub-Committee

The Technical Review Sub-Committee (TRC) shall:

- Act as a control gate within the HUD PPM life cycle to ensure that unnecessary or emerging technical and technology risks and barriers do not prevent the successful production of project deliverables.
- Conduct periodic control gate or milestone reviews and make recommendations based on analyzing or assessing IT investments for technical and technological maturity, feasibility, and technical risk on cost and schedule.
- Act as technical, project, and architecture subject matter experts (SME) for other IT governance bodies as needed to convey present or emerging technical and technology risks and issues.
- Large Projects: Evaluate the alignment of IT projects from technical and technological risk perspectives for HUD's enterprise and segment architecture.
- Small Projects: Evaluate and implement actions as authorized to align segment architecture based on analyses and findings of technical and technology risk.
- Work with the OCIO and other agency units and mission areas in a coordinated effort to help identify, eliminate, or reduce agency-related risks from a technical and technology perspective related to financial management and mission delivery.
- Recommend IT investments for corrective action that exceed or present excessive risk or material and adverse impacts on cost and schedule from a technical or technology perspective.

Project Sponsors and Project Managers

Project Sponsors and Project Managers shall:

- Consider investment risk when making portfolio recommendations.
- Assess, evaluate, and mitigate risks on projects.
- Manage the risk logs or registers.

Investment Owners

Investment Owners shall identify and consider risks when making investment decisions.

Appendix A. Authorities and References

Authorities:

- Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. 113-283, December 18, 2014

- Federal Managers Financial Integrity Act (FMFIA) of 1982, Pub. L. 97-255, 31 U.S.C. § 3512, September 8, 1982

- General Services Administration, *FedRAMP Continuous Monitoring Performance Management Guide version 2.1*. Washington, DC: GSA, February 21, 2018

- Government Accountability Office, *Standards for Internal Control in the Federal Government* (“*Green Book*”), GAO-14-704G. Washington, DC: GAO, September 2014

- Government Performance and Results Modernization Act of 2010, Pub. L. 111-352, January 4, 2011

- HUD Directives System, Handbook No. 000.2 Rev. 3. Washington, DC: HUD, March 2012

- HUD ITM Framework Overview. Washington, DC: HUD, February 10, 2011

- HUD OCIO Issue Management: Quick Reference Guide to Managing IT Project Issues, version 2.0. Washington, DC: HUD, February 2018

- HUD OCIO Risk Management: Quick Reference Guide to Managing IT Project Risks, version 2.0. Washington, DC: HUD, February 2018

- HUD Policy for Information Technology Management, Handbook No. 3400.1, version 1.0. Washington, DC: HUD, April 2011

- HUD Policy for Project Planning and Management, version 2.0. Washington, DC: HUD, January 2017

- National Institute of Standards and Technology, *Contingency Planning for Federal Information Systems*, NIST SP 800-34 revision 1. Washington, DC: NIST, September 2012

Authorities:

- National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. NIST SP 800-37 revision 1. Washington, DC: NIST, June 5, 2014

- National Institute of Standards and Technology, *Guide for Conducting Risk Assessments*, NIST SP 800-30 revision 1. Washington, DC: NIST, September 2012

- National Institute of Standards and Technology, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, NIST SP 800-137. Washington, DC: NIST, September 2011

- National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53 revision 4. Washington, DC: NIST, January 2014

- Office of Management and Budget, *Management's Responsibility for Enterprise Risk Management and Internal Control*, OMB Circular No. A-123. Washington, DC: OMB, July 15, 2016

- Program Management Improvement and Accountability Act of 2015, Pub. L. 114–264, December 14, 2016

References:

- Cutri, David L., *What are (Internal) Controls? Internal Controls and You: Risk Assessment and Risk Management Training*, 23. Toledo, OH: University of Toledo Audit Department. Retrieved at https://www.utoledo.edu/offices/internalaudit/ pdfs/internalcontrolsandyou.pdf

- Gumz, Joy, *Help! Your project has been selected for an audit—what now?* PMI Global Congress 2006 – EMEA, Madrid, Spain. Newtown Square, PA: PMI, 2006

- HUD IT Management Framework Concept of Operations (CONOPS). Washington, DC: HUD. Retrieved at https://www.hud.gov/program_offices/cio/ITMHOME/Conops

- Project Management Institute, *A Guide to the Project Management Body of Knowledge* (6th ed.), 395, 397, 409, 702-722. Newtown Square, PA: PMI, 2017

References:

- Project Management Institute, *Agile Practice Guide*, 151. Newtown Square, PA: PMI, 2017

- Project Management Institute, *Practice Standard for Project Risk Management*. Newtown Square, PA: PMI, 2009

- Risk evaluation, BusinessDictionary.com. WebFinance, Inc. Retrieved at http://www.businessdictionary.com/definition/risk-evaluation.html

- Royer, Paul S. *Project Health Assessment*. Boca Raton, FL: CRC Press, 2015

Appendix B. Definitions

Term	**Definition**
Green Book	a GAO publication, *Standards for Internal Control in the Federal Government*, that provides information about standards, guidance, and a framework for designing, implementing, and operating effective and efficient internal control systems at Federal agencies
Information Technology Management Framework	a set of policies, procedures, standards, and guidelines that help HUD’s customers improve mission delivery of information technology products and services
Internal control	a policy, procedure, and business practice put in place to reduce the chance or likelihood of occurrence for an identified risk
Impact	the costs and effects of an identified risk if it occurs on objectives of an investment, a project, or an organization
Issue	a current condition, event, factor, or situation or an identified risk that has occurred or will occur (that is, occurrence at 100 percent) that has or can have an impact on the objectives of the IT investment, project, or an organization
Information system	a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (NIST SP 800-30)
Portfolio	projects, programs, subsidiary portfolios, and operations that are managed as a group to achieve strategic objectives
Probability	the chance or likelihood and frequency that a risk may occur based on a set of assumptions, data, and information
Program	related projects, subsidiary programs, and program activities that are managed in a coordinated manner to obtain benefits not available from managing them separately

Term	Definition
Project	an effort that involves executing a series of related tasks and activities within a defined scope and assigned resources to achieve planned objectives by creating or producing a unique product, service, or result within a defined start and end date
Project Planning and Management Framework	a set of policies, procedures, standards, and guidelines that provides approaches to optimize innovation, minimize schedule and budget risk, and to plan and execute projects better
Risk	an uncertain, future condition, event, or factor that, if it occurs, may or will have negative or a positive effect on one or more objectives for an IT investment, portfolio, program, project, or an organization
Risk assessment	the process of identifying, measuring, and analyzing internal and external, and controllable and uncontrollable risks at the investment, portfolio, program, and/or project levels and at the enterprise or organizational level
Risk evaluation	the process of estimating the size, occurrence, and effects of the effectiveness of an approach to managing an identified risk; also, the practice of estimating or measuring the size, occurrence, and observed effects on an event or condition in managing a risk management approach on an identified risk
Risk identification	the process of identifying individual project risks, as well as sources of overall project risk and documenting their characteristics
Risk management	the process of identifying, assessing, evaluating, and responding to risks for an IT program or project
Risk Management Plan	a component of a portfolio, program, or project management plan (such as a Program Management Plan, Project Management Plan, or Project Oversight Plan) that describes the process of how risk management activities will be planned and performed for an IT program or project
Risk mitigation	the process of applying a response strategy to reduce the likelihood or probability of occurrence and the effects or impact of a risk

Term	Definition
Risk owner	the person (or persons) who is responsible for monitoring identified risks and for selecting and applying suitable response strategies for those risks

Appendix C. Acronyms and Abbreviations

Abbreviation	Definition
CONOPS	Concept of Operations
EMEA	Europe, Middle East, and Africa
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act
FMFIA	Federal Managers Financial Integrity Act
GAO	Government Accountability Office
GPRA Modernization Act	Government Performance and Results Modernization Act
GSA	General Services Administration
HUD	Department of Housing and Urban Development
ISCM	Information Security Continuous Monitoring
IT	Information technology
ITM	Information Technology Management
LAN	Local area network
NIST	National Institute of Standards and Technology
No.	Number
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OSPM	Office of Strategic Planning and Management
PM	Project Manager
PPM	Project Planning and Management

Abbreviation	**Definition**
PRMB	Performance and Risk Management Branch
Pub. L.	Public Law
SME	Subject matter expert
SP	Special Publication
TRC	Technical Review Sub-Committee
U.S.C.	United States Code of Regulations