Chapter 8
Auditing IT Applications for Risk Management and Strategic Optimization

Varun Razdan
https://orcid.org/0009-0002-7069-2009
University at Buffalo, SUNY, USA

Aman Modi
University at Buffalo, SUNY, USA

Dinesh Kanna Aranganathan
https://orcid.org/0009-0007-3117-0538
University at Buffalo, SUNY, USA

Manish Gupta
University at Buffalo, SUNY, USA

Raj Sharman
https://orcid.org/0000-0001-5838-7330
University at Buffalo, SUNY, USA

ABSTRACT

This chapter presents a comprehensive strategy for auditing IT application portfolios to mitigate risks, enhance governance, and drive strategic optimization. Targeted at IT auditors, risk professionals, and enterprise architects, it integrates frameworks such as CISA, COBIT, ITIL, SOC 2, NIST, and ISO 27001 to guide practices in inventory validation, business alignment, cost-effectiveness, technical risk, and cloud readiness. Structured tools like checklists, the TIME model, and dashboards support a systematic audit process. A hypothetical case study illustrates practical

DOI: 10.4018/979-8-3373-3078-5.ch008

application across multi-industry and multi-region settings, demonstrating how audit-driven insights can uncover redundancies, improve lifecycle health, and strengthen operational resilience. This chapter per the authors emphasizes that a well-governed application portfolio audit not only ensures compliance and risk mitigation but also enables substantial cost savings and better alignment with modernization goals.

INTRODUCTION

Modern enterprises rely on a vast array of software applications to support business processes, but unmanaged growth of the application portfolio can lead to *application sprawl* – duplicated functions, rising costs, and increased operational risk (Theseira, 2024; Faddom, 2023). *Application Portfolio Management (APM)* is the discipline that governs applications throughout their lifecycle to maximize business value delivery (Global Affairs Canada, 2022). Effective APM involves maintaining a comprehensive inventory of applications and continuously assessing each for its business value, technical health, cost, and risk, so that informed decisions can be made on which applications to **keep, modernize, or eliminate** (Global Affairs Canada, 2022; CIO Council & C&I CoP, 2020). In practice, however, many organizations struggle with incomplete application inventories, siloed ownership, outdated systems, and misaligned resources, prompting the need for rigorous auditing of the application portfolio.

Auditing an IT application portfolio is a systematic approach to evaluating how well an organization catalogs, governs, and optimizes its software applications. Unlike a one-time project, portfolio auditing is often a continuous or periodic activity woven into IT governance and risk management programs (Theseira, 2024). The goal is twofold: **assurance** – verifying that controls and best practices are in place for managing the portfolio, and **advisory** – identifying opportunities to streamline and enhance the portfolio for better business alignment and cost-effectiveness.

This paper examines strategies for auditing application portfolios effectively. It bridges *practical techniques* (like inventory validation, scoring models, and tool-supported analysis) with *theoretical frameworks* that auditors and IT managers commonly use. Frameworks such as ISACA's CISA and COBIT 2019, ITIL 4's Portfolio Management practice, AICPA's SOC 2 trust principles, NIST's Cybersecurity Framework and Risk Management Framework, and ISO/IEC 27001's controls on asset management all inform the standards for a well-governed application portfolio. By aligning the audit approach with these recognized frameworks, auditors can ensure comprehensive coverage of governance, risk, and compliance aspects (Wiseman, 2025).