

# Case Study: Information Technology Controls in a Governmental Environment

Information technology (IT) controls are the policies, procedures, and practices that ensure the confidentiality, integrity, and availability of information systems and data. IT controls are essential for any organization, but especially for governmental entities that handle sensitive and confidential information, such as personal records, financial transactions, national security, and public services. IT controls can be classified into two categories: general controls and application controls. General controls apply to the overall IT environment and affect all systems and data, such as access control, change management, backup and recovery, and security monitoring. Application controls apply to specific processes or systems and ensure the accuracy, completeness, and validity of inputs, outputs, and processing, such as data validation, transaction authorization, and error detection.

In this case study, we will examine the IT controls of a hypothetical governmental agency, the Department of Education (DoE), and identify the associated risks, challenges, and best practices. The DoE is responsible for overseeing and funding educational programs, conducting research and evaluation, and enforcing civil rights laws related to education. The DoE relies on various IT systems to support its mission and operations, such as the Federal Student Aid (FSA) system, which manages financial aid for students; the National Center for Education Statistics (NCES) system, which collects and analyzes data on education; and the Office for Civil Rights (OCR) system, which handles complaints and investigations of discrimination. The DoE also uses a common IT infrastructure, such as networks, servers, databases, and email, to facilitate communication and collaboration among its staff and stakeholders.

## Cybersecurity Threats

The DoE is constantly exposed to cyberattacks from various sources, such as hackers, criminals, domestic and foreign adversaries, and insiders, who may attempt to compromise, steal, or destroy the DoE's data and systems. For example, in 2022, the DoE reported a breach of the FSA system that affected about 100,000 taxpayers who applied for financial aid using an online tool linked to the Internal Revenue Service (IRS). The attackers exploited a vulnerability in the tool and accessed personal information, such as names, addresses, Social Security numbers, and tax return data. The DoE had to suspend the tool, notify the affected individuals, and provide identity protection services and fraud prevention measures.

## Compliance Requirements

The DoE has to comply with various laws and regulations that govern its IT activities, such as the Federal Information Security Management Act (FISMA), which requires federal agencies to implement and assess IT security programs; the Privacy Act, which protects the privacy of individuals' records maintained by federal agencies; and the Family Educational Rights and Privacy Act (FERPA), which protects the privacy of students' education records. The DoE must also follow the standards and guidelines issued by the National Institute of Standards and Technology (NIST),

which provide recommendations> for IT security and control. The DoE has to report on its compliance status and performance to the Office of Management and Budget (OMB), the Government Accountability Office (GAO), and other oversight bodies and respond to audits and reviews.

## Resource Constraints

Given the limited budget and personnel available, the DoE has to manage its IT resources efficiently and effectively. The DoE has to prioritize its IT investments and projects based on alignment with its strategic goals and objectives, as well as the expected costs and benefits. The DoE also has to ensure that its IT staff have the necessary skills and competencies to perform their roles and responsibilities and provide training and development opportunities. Moreover, the DoE has to coordinate and collaborate with other federal agencies, state and local governments, educational institutions, and private sector partners, who may have different IT systems and standards.

To address these risks and challenges, the DoE has implemented several IT control best practices, such as:

- **Risk management:** The DoE has established a risk management framework and process that identifies, analyzes, evaluates, and responds to IT-related risks. The DoE conducts regular risk assessments and audits to evaluate the effectiveness of its IT controls and identify any gaps or weaknesses. The DoE also develops and updates its contingency plans and disaster recovery plans to ensure the continuity of its critical operations and services during a disruption or emergency.
- **Governance and oversight:** The DoE has established a governance and oversight structure and mechanism that defines the roles and responsibilities of various stakeholders involved in IT decision-making and oversight. The DoE has a Chief Information Officer (CIO) who is responsible for leading and managing the DoE's IT functions and activities and ensuring compliance with IT policies and standards. The DoE also has an IT Steering Committee, which consists of senior executives from different offices and programs, and provides strategic direction and guidance for IT initiatives and investments. The DoE also has an IT Security Council, which consists of representatives from different business units and functions, and advises on IT security issues and solutions.
- **Control monitoring and evaluation:** The DoE has established a control monitoring and evaluation system and process that measures and reports on the performance and effectiveness of its IT controls. The DoE uses various tools and methods to monitor and evaluate its IT controls, such as self-assessments, audits, reviews, inspections, tests, and surveys. The DoE also uses various metrics and indicators to track and report on its IT control outcomes and impacts, such as security incidents, system availability, customer satisfaction, and cost savings. The DoE also implements corrective actions and improvements based on the findings and recommendations of its control monitoring and evaluation activities.

## Assignment

Identify specific examples of technology-focused internal controls that should be in place at the DOE to mitigate risk to a prudently acceptable level. Categorize each internal control procedure as being one of the following control types:

1. Preventive control
2. Detective control
3. Deterrent control
4. Compensating control

## Summary

This case study illustrates the importance and complexity of IT controls in a governmental environment and highlights the associated risks, challenges, and best practices. By implementing effective IT controls, the DoE can enhance its ability to achieve its mission and objectives and protect its data and systems from unauthorized access, use, disclosure, modification, or destruction. IT controls can also help the DoE improve its efficiency and effectiveness and comply with various laws and regulations governing its IT activities.