AUDIT
REPORT

Information Technology General Controls

JANUARY 2025

TIMOTHY M. O'BRIEN, CPA
DENVER AUDITOR

OFFICE OF THE AUDITOR
AUDIT SERVICES DIVISION, CITY AND COUNTY OF DENVER

Audit Team

Peter Ulrich, CISA, CSX-A, Information Systems Audit Manager
Nicholas Jimroglou, CISA, CDPSE, Information Systems Audit Lead
Dave Hancock, CISA, CISM, MURP, Information Systems Audit Senior

Other Contributors

Stelios Pavlou, Communication and Reporting Specialist
Manda Troutman, Communication and Reporting Specialist
Jeff Neumann, Graphics and Visual Information Specialist

Audit Managers

Timothy M. O'Brien, CPA, Auditor
Valerie Walling, CPA, Deputy Auditor
Dawn Wiseman, CRMA, Audit Director

Audit Committee

Timothy M. O'Brien, CPA, Chairman
Jack Blumenthal, Vice Chairman
Frank Rowe
Leslie Mitchell
Florine Nath
Charles Scheibe
Ed Scholz

You can obtain copies of this report by contacting us.

Office of the Auditor
201 West Colfax Ave. #705
Denver, CO 80202
(720) 913-5000

Or download and view an electronic copy by visiting our website at: www.DenverAuditor.org.

Response narratives are reprinted verbatim from the agency's letter, which is available in full on our website.

Cover photo illustration by Denver Auditor's Office staff.

TIMOTHY M. O'BRIEN, CPA
AUDITOR

201 West Colfax Ave. #705, Denver, CO 80202
(720) 913-5000 | www.DenverAuditor.org

AUDITOR'S LETTER

January 16, 2025

We audited an agency in the City and County of Denver. This assessment found some areas of strength and some areas that need improvement. Because of the information security sensitivities involved with this assessment, we have communicated these issues separately to the relevant city agency for its remediation.

This assessment is authorized pursuant to the City and County of Denver Charter, Article V, Part 2, Section 1, "General Powers and Duties of Auditor."

We extend our appreciation to the city personnel who assisted and cooperated with us during the assessment. For any questions, please feel free to contact me at 720-913-5000.

Denver Auditor's Office

Timothy M. O'Brien, CPA
Auditor

BACKGROUND

Information technology general controls

Based on information from the Institute of Internal Auditors, information technology general controls are defined as a set of processes, procedures, and standards that support the use of technology in the organization while managing, protecting, and governing the systems, applications, data, and processes from failure and inconsistent performance.

Figure 1 shows information technology general controls in the following categories and a high-level description of the control objectives:

FIGURE 1. Information technology general controls by category

ASSET MANAGEMENT	USER LIFECYCLE MANAGEMENT	DATA PROTECTION	INFORMATION TECHNOLOGY OPERATIONS	INTERFACE CONTROLS	CHANGE CONTROLS	APPLICATION DEVELOPMENT	CYBER RESILIENCE
The process of managing hardware and software through its lifecycle.	The process to ensure only allowed people and processes have access to hardware, systems, data, and processes.	The process to ensure an organization's data is controlled and managed to ensure it is used for a specific business purpose.	The day to day maintenance to ensure applications, systems, and data are available.	The process to ensure data is moved completely and accurately across infrastructure.	The processes to ensure changes to systems and data are properly governed, tested, and approved.	The process to ensure only properly developed internal applications are taken on as projects by the organization.	The processes to ensure an organization can respond to and recover from an incident or disaster.

Source: *Created by Auditor's Office staff.*

Information technology general controls are considered the building blocks and minimum standards to ensure information technology systems can maintain confidentiality, integrity, and availability. The National Institute of Standards and Technology defines these terms as:

- **CONFIDENTIALITY** – preserving authorized restrictions on information access and disclosure, including the means of protecting personal privacy and proprietary information.
- **INTEGRITY** – guarding against improper information modification or destruction and ensuring information nonrepudiation and authenticity.

- **AVAILABILITY** – ensuring timely and reliable access to and use of information.

NONREPUDIATION

The National Institute of Standards and Technology defines nonrepudiation as, "In a general information security context, assurance that the sender of information is provided with proof of delivery, and the recipient is provided with proof of the sender's identity, so neither can later deny having process the information."

Without effective information technology general controls an organization may not be able to achieve its objectives. This may result in the loss of public trust, data breaches, and financial penalties.

Identity and access management lifecycle

Gartner defines identity and access management as "a security and business discipline that includes multiple technologies and business processes to help the right people or machines to access the right assets at the right time for the right reasons, while keeping unauthorized access and fraud at bay." This process ensures the right digital identities can access, create, update, delete, and read data to maintain the confidentiality, integrity, and availability of the organization's applications and systems.

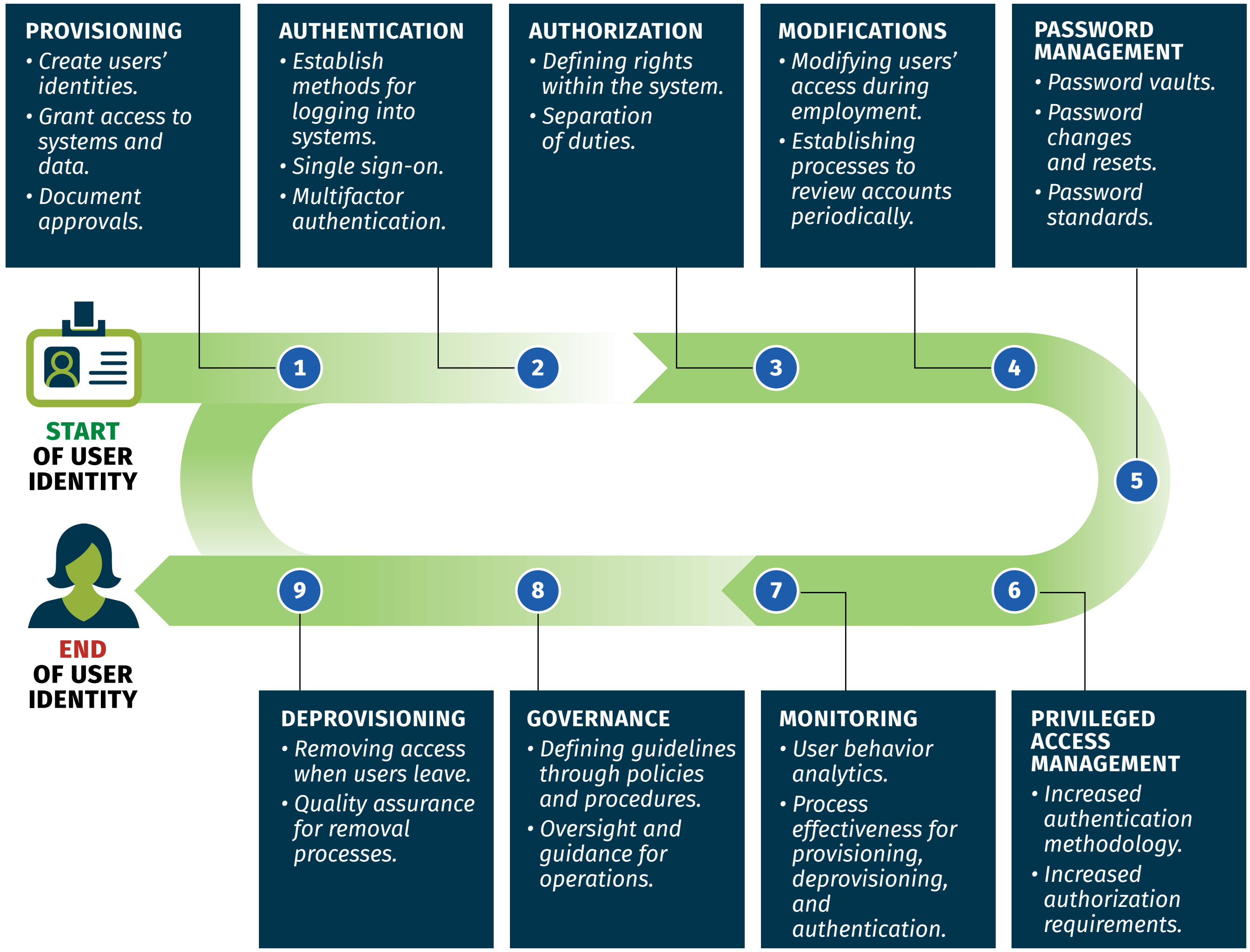
The Center for Internet Security's "Top 18 CIS Critical Security Controls" provides more specific actions for organizations to take to effectively manage the identity management lifecycle. Control 5 on the list focuses on account management, while Control 6 centers on access control management. These two controls make up a significant amount of the identity and access management process.

On the next page, Figure 2 shows the processes necessary to effectively manage an organization's digital identities.

DIGITAL IDENTITIES

SailPoint, an industry leader in identity and access management, defines a digital identity as "an individual's digital version of their analog identity. It consists of multiple accounts, credentials, entitlements, behaviors, and usage patterns associated with an individual. Represented and digitally documented online, a digital identity provides a digitally authenticated and stored collection of characteristics associated with a uniquely identifiable individual. It is used to authenticate users when validated proof of identity is required to access online services or perform transactions or operations."

FIGURE 2. Identity lifecycle management



Source: *Auditor's Office recreation of information from Collidu.com.*

Effective identity and access lifecycle management is an important control process required by most standards and certification bodies. The risk of an ineffective process includes:

- Unauthorized access.
- Insider threats.
- Data breaches.
- Financial losses.
- Operational disruptions.
- Compliance violations.
- Reputational damage.

Organization should dedicate sufficient resources to ensure these risks are managed using controls established by organizations such as the National Institute of Standards and Technology, the Center for Internet Security, or other standard setting bodies.

According to the "Verizon 2024 Data Breach Investigations Report," 24% of all breaches in 2024 involved bad actors using stolen usernames and passwords to break into systems. Proper username and password management is a key component of identity and access management.

Cyber resilience

When a breach occurs, an organization's ability to detect, respond to, and recover from the breach is critical to ensuring operations continue with minimal interruptions.

The National Institute on Standards and Technology defines cyber resiliency as, "The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment."

The National Institute of Standards and Technology created "The NIST Cybersecurity Framework (CSF) 2.0" to help organizations implement processes to ensure they can govern, identify, protect, detect, respond to, and recover from a cybersecurity event.

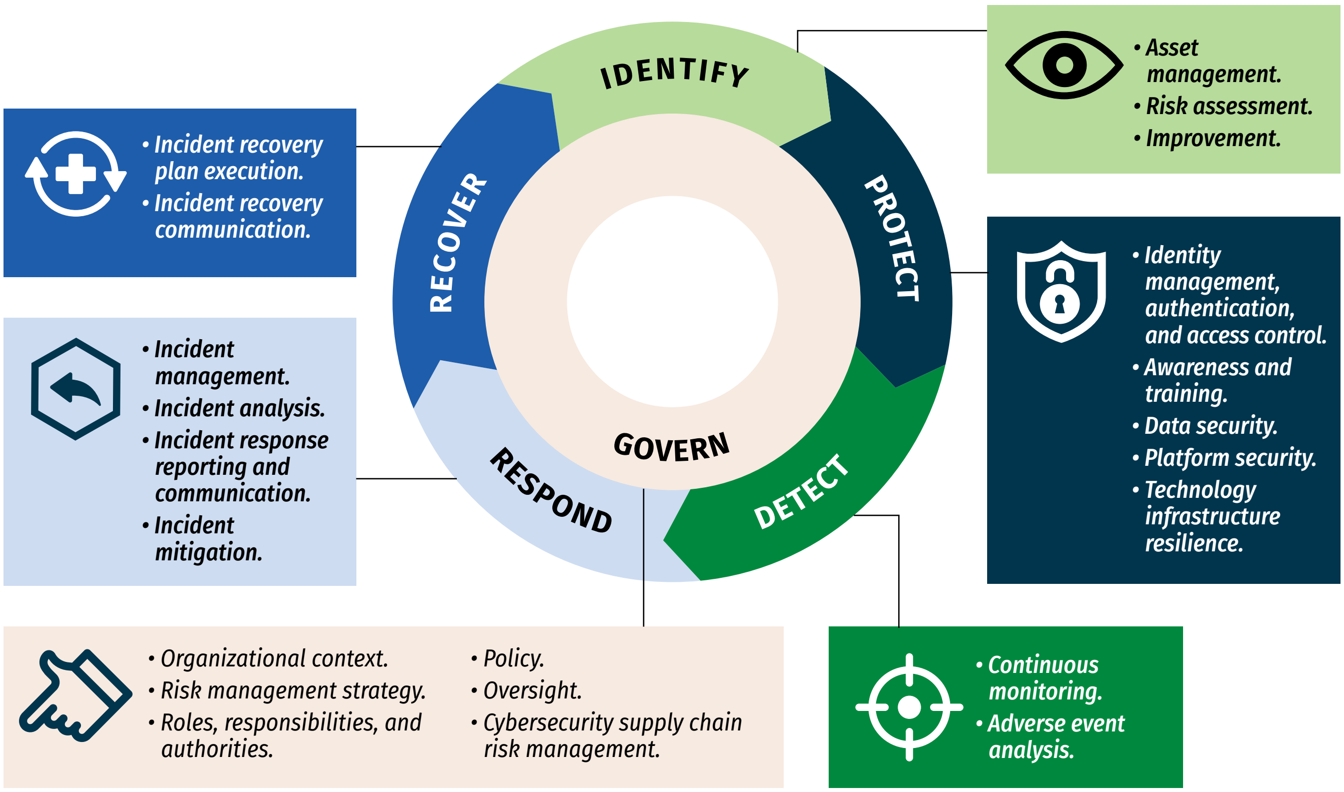
On the next page, Figure 3 describes each of the significant processes in the cybersecurity framework.

According to the Identity Theft Resource Center's "2023 Data Breach Report," there were 3,205 cyberattacks in 2023, with 353,027,892 victims. IBM estimates the average cost of a breach is $4.88 million and organizations should take action to implement and sustain cybersecurity processes. The risks of not having effective cyber resiliency processes include:

- Increased vulnerability to cyberattacks.
- Increased business disruption.
- Reputational damage.
- Increased costs.
- Regulatory noncompliance.

Organizations with effective cyber resiliency programs are more effective in achieving their goals because they will not spend as much time working on, responding to, and recovering from cyber security events compared to unprepared organizations.

FIGURE 3. Cyber resilience framework



Source: *Created by Auditor's Office staff based on National Institute of Standards and Technology guidance.*

Mobile device management

As organizations adjust to a remote or hybrid workforce that relies on mobile devices to stay connected and engaged in day-to-day operations, the need to find ways to control employees' work behavior on their mobile devices increases in importance.

According to SlashNext's "2023 Mobile BYOD Security Report," 85% of employers require work-related applications to be installed on employees' personal devices. And 71% of those users store sensitive work passwords on that device. IBM defines BYOD as, "Bring your own device means employees use their personal mobile devices for work instead of company-issued devices."

Based on the risk of an employee accessing or using sensitive data on their phones, businesses need to implement mobile device management solutions to protect both the employee and the organization from unintentional data leaks or exposure.

The most widely accepted way to control how employees use company resources on their personal devices is through a mobile device management tool.

The National Institute of Technology and Standards defines mobile device management as, "The administration of mobile devices such as smartphones, tablets, computers, laptops, and desktop computers. Mobile Device Management is usually implemented through a third-party product that has management features for particular vendors of mobile devices."

Mobile device management tools, which are installed on employees' mobile devices, help ensure organizations comply with their specific security, data, and privacy requirements. When installed and properly configured, mobile device management tools offer several functions:

- Device tracking.
- Capability management.
- Application security.
- Remote wiping.
- Identity and access management.
- End point security.

By ensuring mobile devices are secured with the same rigor as laptops and other hardware, an organization can help limit its risk exposure from:

- Data leakage.
- Malicious or unapproved applications.
- Device infections.
- Mixing personal and business use.
- Inability to manage devices.

By implementing, properly configuring, monitoring, and ensuring a mobile device management tool is installed on all of an organization's mobile devices, the organization can limit the potential risks associated with using a mobile device for work. Without a mobile device management solution, the organization may be exposing its data and applications to bad actors — potentially leading to financial loss, regulatory noncompliance, brand damage, and data leaks.

Office of the Auditor

The **Auditor** of the City and County of Denver is independently elected by the residents of Denver. He is responsible for examining and evaluating the operations of city agencies and contractors for the purpose of ensuring the proper and efficient use of city resources. He also provides other audit services and information to City Council, the mayor, and the public to improve all aspects of Denver's government.

The **Audit Committee** is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities regarding the integrity of the city's finances and operations, including the reliability of the city's financial statements. The Audit Committee is structured in a manner that ensures the independent oversight of city operations, thereby enhancing residents' confidence and avoiding any appearance of a conflict of interest.

201 West Colfax Avenue, #705

Denver, CO 80202

(720) 913-5000

www.DenverAuditor.org

Our Mission

We deliver independent, transparent, and professional oversight in order to safeguard and improve the public's investment in the City and County of Denver. Our work is performed on behalf of everyone who cares about the city, including its residents, workers, and decision-makers.