,,

Computer Science-A.I.

APPLICATION OF GOVERNANCE ON THIRD-PARTY IDENTITIES

Cem Ayerdem 2690713

Supervisor:
Dr. Olga Gadyatskaya

BACHELOR THESIS

Leiden Institute of Advanced Computer Science (LIACS)
www.liacs.leidenuniv.nl

21/05/2025

Abstract

Third-party identity governance is an important aspect of access management, where technologies and policies ensure that only authorized users can access specific resources within an institution. As a pivotal component of Identity and Access Management (IAM) within cybersecurity, many advances have been made. However, current practices across companies often fail to mitigate the risks associated with third-party access [IBM24]. Additionally, there is a limited recognition to the extent of the problem.

This issue came to light during a professional project, which revealed major challenges in the management of third-party identities. These identities, representing external collaborators and service providers, often lack proper governance structures. Inadequate management leads to insufficient oversight, increased security vulnerabilities, non-compliance with regulatory requirements, and even reputational damage.

This thesis investigates the impact of these oversight gaps through observational data from real-world scenarios. The primary contribution of this study is the development of a conceptual framework and classification system to establish a systematic foundational approach for the governance of third-party identities. Since comprehensive governance is a broad and complex system, these contributions are intended to serve as a foundation for building a more robust governance structure. The proposed framework leverages insights from both fieldwork and industry practices to ensure practical applicability and relevance.

By addressing the impact of lacking oversight through fieldwork and real-world observations, this research contributes to a deeper understanding of the complexities surrounding third-party identity governance. The findings aim to inform strategies that enhance the safety and effectiveness of governance frameworks, ultimately improving their quality.

Contents

1 Introduction

1.1 Research Problem and Motivation

In today's digital world, businesses work closely with outside partners like vendors, contractors, and service providers. These partnerships help companies grow and run smoothly. However, they also come with risks, especially when third-party access to company systems isn't properly managed. Unlike employee accounts, which follow clear rules for setup and removal, third-party accounts often don't have the same level of control. This can lead to accounts staying active long after they're needed, giving people more access than they should have, and even causing security and compliance issues. For example, a company hires a contractor for a short-term project. To get their work done, the contractor is given access to certain company systems. When the project ends, their access should be removed immediately. Nevertheless, this does not happen in many cases. Their account stays active, becoming an easy way for cybercriminals to break in. In 2024, a CyberArk report [Cyb24] found that 93% of companies had security breaches linked to identity issues, and 83% of those were due to improperly managed third-party accounts.

These mistakes can be expensive. According to IBM's 2024 data breach report [IBM24], Security failures cost organizations an average of 4.88 million dollars per breach, making weak identity governance a major financial and security risk. The IBM report found that breaches involving stolen credentials take the longest to detect and contain 292 days on average even longer than phishing 261 days and social engineering 257 days.

If regular account-based attacks already take this long to resolve, third-party accounts often overlooked and poorly managed are likely even more risky. These accounts frequently are overpriviliged and remain active longer than necessary, making them an ideal target for attackers. Without automated deprovisioning and continuous monitoring, third-party identities can lead to extended unauthorized access and increased breach costs. This highlights the urgent need for stronger governance.

Most companies use Identity and Access Management (IAM) systems to control who can access their internal systems. These systems work well for employees because they follow a structured process called the Joiner, Mover, Leaver (JML) lifecycle [CG22], as illustrated in Figure 1.:

- **Joiner**: When a new employee is hired, they get an account with the right level of access.
- **Mover**: If the employee's job changes, their permissions are updated.
- **Leaver**: When an employee leaves the company, his/her access is removed to keep the system secure.

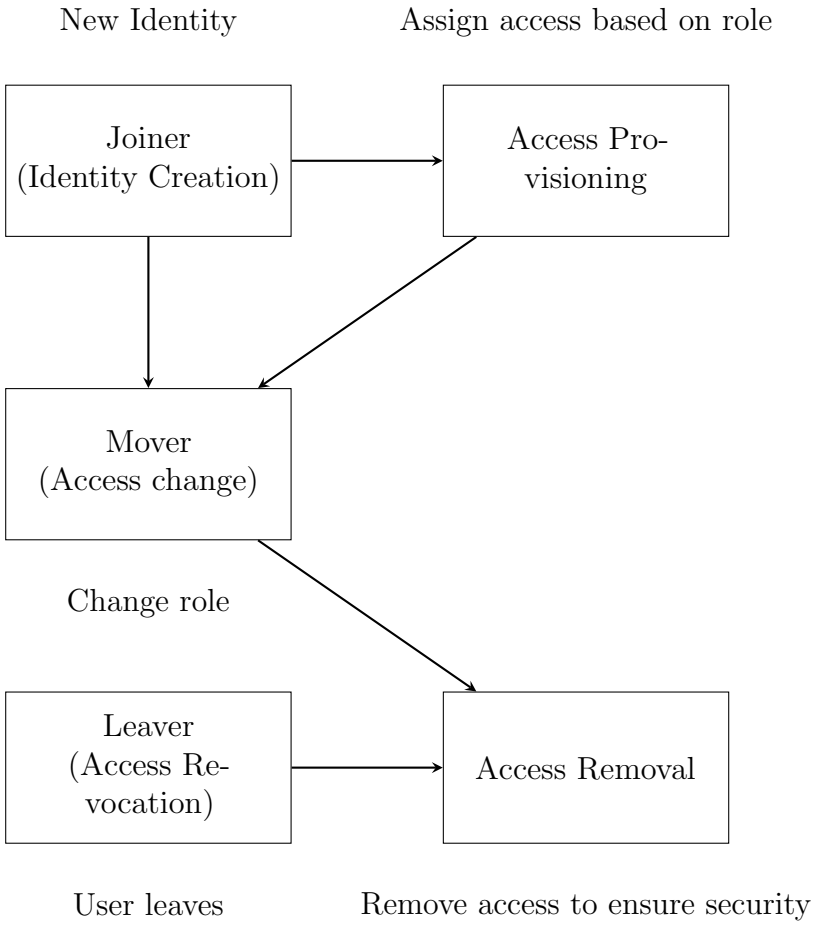

Figure 1. The Joiner, Mover, Leaver (JML) Process for Traditional Identities

This process makes sure that employee accounts are well-managed, however third-party accounts do not follow the same rules. A 2024 SailPoint report [Tec24] found that 41% of organizations remain at the lowest level of identity security maturity, indicating significant challenges in managing identities, including third-party identities , often leaving accounts active for too long and creating security risks. Contractors, vendors, and service providers are usually given temporary access, though their accounts are not always tracked or removed when they should be. Without proper management, these accounts can lead to unauthorized access, legal problems, and even damage to a company's reputation.

The governance of third-party identities presents several challenges. Firstly, there are inconsistent policies for account management. Many organizations lack clear guidelines for creating, modifying, or deactivating third-party accounts. This inconsistency leads to floating accounts that pose security vulnerabilities. In addition, third-party identities are overprivileged. This means that third-party users are often granted more access than necessary. Subsequently, this increases the risk of unauthorized access to critical systems and sensitive data.

Furthermore, since there is an absence of effective monitoring tools, tracking third-party activities remains difficult, leaving misuse or anomalies undetected.

Moreover, there is a lack of specialized tools. Since most IAM systems are designed for internal use, they do not address the dynamic and temporary nature of third-party accounts effectively. These challenges highlight the need for a governance framework tailored specifically to third-party identities.
To fix these issues, companies need a better way to manage third-party accounts, which will be further explained in this thesis.
This thesis focuses on creating a better way to manage third-party accounts by developing a Third-Party Identity Governance (TPIG) framework based on insights from work experience and cases within a cybersecurity consultancy firm. The goal is to close the gaps in current IAM systems by standardizing how third-party identities are created, tracked, and removed. By improving security and automating key processes, companies can better protect their systems while still working efficiently with external partners.

1.2 Scientific Relevance

This research advances the field of cybersecurity by addressing the gaps in third-party identity governance. The key contributions of this study include defining the problem, secondly, identifying weaknesses in current IAM systems which fail to manage third-party access resulting in security vulnerabilities. Additionally, real-world breaches will be analyzed by examining case studies of past security incidents to uncover common risk patterns caused by poor third-party identity management. Ultimately, a governance framework will be developed which will propose an improved framework that extends IAM principles to third-party identities, integrating stricter access control, real-time monitoring, and automated lifecycle management. Lastly, a risk-based categorization model will be introduced as a system that classifies third-party identities based on factors like trust level, access scope, and compliance requirements, helping organizations apply more effective security measures. By combining theoretical cybersecurity principles with real-world applications, this study enhances both academic research and practical cybersecurity strategies.

1.3 Security Science Context

This research falls under cybersecurity governance, with a focus on identity management, access control, and risk mitigation. Security science in the context of this thesis involves using structured methodologies and frameworks to protect digital identities and reduce cyber risks. By integrating security policies, automated monitoring, and zero-trust principles, this study enhances our understanding of how organizations can systematically govern third-party identities. Also, the research aligns with industry standards such as NIST and modifies the Data Governance Institute (DGI) framework to better fit third-party identity management challenges [Nat18] [Ins24]

2 Literature Review and Research Gap

2.1 Background on Identity and Access Management (IAM)

Effective cybersecurity frameworks rely on robust Identity and Access Management (IAM) systems. It makes sure that the right people can access the right tools or data at the right time, and for the right reasons [McK21]. Traditional Identity and Access Management (IAM) systems are well-established for internal employees to handle things like logging in (authentication), giving permissions (authorization), and managing accounts. According to Mohammed et al., [Moh17] IAM is a key part of cybersecurity with three main points: data security, provisioning, and compliance. This review concluded that poorly set up access rights (provisioning) and unclear role structures especially in environments where identities are harder to monitor are common problems which are not yet solved, and it also emphasized that IAM isn't only about security, but it also helps organizations work more efficiently by automating account creation and removal with the joiner-mover-leaver [CG22]. Focusing more on the foundational components and operational challenges, Mandru et al., [Man19] narrowed the scope to critically assess one of IAM's core models Role-Based Access Control (RBAC) in large enterprise IAM systems. The study concluded that RBAC is scalable and easier to audit compared to older models like Discretionary Access Control (DAC) or Mandatory Access Control (MAC) and suggested in order to simplify role management, hybrid models and automated role mining tools should be applied.
However, his study focuses mainly on internal employees and does not explore how RBAC could be adapted for third-party users, who often do not fit neatly into predefined roles. Recent studies also have shown that IAM is changing and needs to become more flexible and adaptable. For example, Glöckler et al., [GSFF23] did a detailed review and found that self-sovereign identity (SSI) could be useful in IAM systems of companies. SSI is a decentralized way of managing identities, where users control their own information instead of relying on a central system. This flexible model can help organizations better manage different types of users and reduce risks tied to single points of failure in traditional systems.

2.2 Identity Governance

In Identity and Access Management (IAM), governance means all the rules, processes and tools used to make sure identities are handled safely and follow legal requirements. Effective identity governance involves not only assigning and managing access rights, but also continuously monitoring and auditing these rights to prevent unauthorized access. Identity governance focuses mostly on answers for questions such as: ''Who has access? Why should they have it? How do we know they should have it?".
Glöckler et al., [GSFF23] conducted a systematic review of IAM challenges and needs in organizations, followed with IAM-expert interviews. Four main requirement areas for Identity and Access Management were identified: Security and Compliance, Manageability and Cost, User Experience, and Technology, and Interoperability. They also built and tested a Self Sovereign Identity (SSI) prototype using a Design Science Research (DSR) approach. Design Science Research (DSR) is a method focused on creating and evaluating practical solutions to real-world problems. It combines building a working prototype with learning from how it performs in practice. SSI lets users store and manage their credentials in a digital wallet, allowing features like passwordless login and privacy

based identity checks.
Their findings showed that while SSI can improve User Experience and make IAM systems easier to manage, SSI still lacks the ability to meet more complex enterprise governance needs, especially in areas such as role management and managing third-party access. This shows that IAM governance is not just about technology, it also requires strong policies, regular checks, automated processes, and clear responsibility for who gets access and why.
The complexity of managing access rights is further highlighted by Baumer et al. [BMHR24] who found that even well-intentioned access review processes often fail due to usability issues. Their study introduced the concept of digital nudges. Digital nudges are subtle design elements in user interfaces that help guide users' decisions without limiting their options. For example, using default settings that suggest removing unnecessary permissions helped reviewers make better decisions during the access review process. This approach not only made the review process more efficient, but also reduced the mental load and stress on the reviewers. Their findings show that effective identity governance is not only a technical issue, but also a human centered one. User interface design and user behavior play a critical role in maintaining access security.

2.3 Third-Party Identity Governance: Current State

IAM frameworks are designed to ensure that only authorized users can access specific organizational resources. Traditional IAM models focus primarily on employees and include mechanisms such as Authentication & Authorization where user verification happens before granting access. Also, Role-Based Access Control (RBAC) where permissions are assigned based on job functions. Lastly, there is Privileged Access Management (PAM) where sensitive resources are protected by restricting high-risk accounts.
However, managing third-party identities such as contractors, vendors and partners brings unique challenges. These external users often need temporary or dynamic access, which traditional IAM models are not built to handle well. RBAC for example, works effectively for managing internal employees by assigning access based on fixed roles. However, it often fails with third-party identities who often require short term access and don't align well with fixed role models. This can lead to issues such as floating accounts, excessive access privileges, and poor oversight [IBM24].
Although security standards such as NIST SP 800-53 and ISO 27001 [Nat18] [Int22] highlight the importance of strong access policies, they offer limited guidance on managing temporary external users. As a result, many organizations struggle to apply consistent identity governance to third-party users.
Some research has started to explore this issue. For example, Xu et al., [XLJ23] proposed a Blockchain based framework that improves transparency and trust in third-party entities. Their model aims to protect privacy while also holding third-party authorities accountable using Blockchain technology. While this is a promising step, there is still no complete academic framework that focuses specifically on the governance of third-party identities revealing a clear gap in current research.

2.4 Key Challenges in Third-Party Identity Management

As mentioned previously, while IAM frameworks are well established for internal users, managing third-party identities require temporary, dynamic access and may operate across organizational boundaries. Traditional IAM models like RBAC and PAM are not built to handle such dynamic and externally managed identities.

Studies highlight several key risks in third-party identity management. One of the most common issues is floating accounts, these are accounts that remain active long after their intended use. A 2024 report by SailPoint found that 41% of organizations experience delays in deactivating third-party accounts, leaving unused credentials vulnerable to misuse [Tec24]. Another major issue is overprivileged access. Research by CyberArk (2024) shows that 82% third-party users have more permissions than needed, increasing the attack surface and the potential for privilege escalation [Cyb24].

The lack of continuous monitoring is an another important challenge as well. IBM's 2024 Cost of a Data Breach Report found that identity related breaches take an average of 292 days to identify and contain, indicating a lack of real-time oversight [IBM24]. Many organizations fail to apply basic security controls like multi factor authentication (MFA) to external users, making them easy targets for attackers. Additionally, compliance frameworks such as GDPR and SOC 2 focus mainly on employee access and offer limited guidance for third-party identity governance [Nat18].

2.5 Existing Solutions and Their Limitations

Current IAM models do not sufficiently address the governance of third-party identities. These external users often have temporary or frequently changing roles, which makes it difficult to assign consistent access rights. They may also need access across different systems or organizations, which makes it harder to keep track of their identities and what they can do. Furthermore, third-party identities are often hard to monitor/move using the traditional joiner-mover-leaver process, which is typically designed for permanent internal employees.

As mentioned, one approach is Role-Based Access Control (RBAC) which assigns permissions based on job functions and helps reduce unauthorized access. It is convenient for it's scalability and ease of auditing when compared to older models like Discretionary Access Control (DAC), where users can decide who else can access their files, and Mandatory Access Control (MAC), where access is tightly controlled by the system based on how sensitive the information is and the user's clearance level [Man19]. Although RBAC provides a more practical and manageable solution for most organizations, it lacks the flexibility required for third-party identities, whose access needs are often temporary and inconsistent. One common issue is role explosion, where too many overlapping roles are created, making the system difficult to manage. Another problem is role rigidity, as static roles often do not work well for short term or dynamic identities. Additionally, manual role assignment can become time consuming if not automated. To address these challenges, hybrid models and automated role mining tools should be applied [Man19]. However, the study mainly focuses on internal users and does not explore how these solutions could be adapted to manage third-party identities.

Privileged Access Management (PAM) is another important tool in IAM. It is effective at securing high-risk accounts by enforcing strong authentication and limiting access to sensitive resources. However, PAM is not well-suited for managing large numbers of temporary third-party users, as it

lacks scalability and flexibility for short-term access needs [Cyb24]
Automated Lifecycle Management is often recommended to streamline the provisioning and deprovisioning of user accounts. Some IAM systems do offer automated processes, but many organizations still rely on manual workflows. This leads to delays in revoking access, increasing the risk of floating accounts and overprovisioned permissions [Tec24]
Glöckler et al., [GSFF23] explored Self-Sovereign Identity (SSI) as a model. SSI allows users to manage their credentials through digital wallets, improving User Experience and reducing reliance on centralized systems. While SSI supports privacy and authentication, it does not fully address enterprise wide governance needs. As noted by Glöckler et al.: *"SSI can specifically improve manageability and usability aspects and help implement acknowledged best practices such as the principle of least privilege"* but it does not solve challenges like access audits, lifecycle management, or access reviews for third-party identities.
Beyond technical models like Role-Based Access Control (RBAC) and Self Sovereign Identity (SSI), access governance also struggles with limited visibility for administrators and a lack of effective tools. Shen et al. [BSZ23] addressed this problem through their development of *SECLOG*, a tool designed to improve access and deny log messages. The tool aids system administrators in avoiding the over-granting permission mistakes. SECLOG uses static analysis to automatically detect access control checks within various server applications, identifying where access and deny logs are missing and what relevant information should be included. By making log messages clearer and more informative, SECLOG helps administrators by making better decisions, thus reducing the risk of unnecessary privilege escalation. The study found that when logging and diagnostic information is insufficient, administrators often escalate privileges by mistake, creating serious security risks.

In summary, while current IAM solutions offer partial answers, they fall short of meeting the specific needs of third-party identity governance. Existing models are not flexible or automated enough to handle the temporary, dynamic, and externally managed nature of third-party access.
There are also numerous commercial solutions available for third-party identity management. However, these tools often exhibit certain limitations. One issue is commercial bias, as many existing solutions are designed to promote specific platforms and tools, which may not always align with the unique needs of every organization. This commercial bias can lead to suboptimal identity governance practices. Moreover, the available solutions are often fragmented, addressing specific aspects of third-party identity management such as access provisioning or monitoring rather than offering a complete, integrated approach.
To identify the tools presented in the following Table, industry consultants were consulted and market research reports on third-party identity governance and risk management were reviewed. This approach combined expert insights and an analysis of widely recognized resources to ensure a thorough overview of available solutions.

A brief analysis of what tools are on the current market:

Tool Name	Description	Link
BitSight	Monitors vendors external-facing identity security posture and highlights risks linked to exposed or weakly protected third-party accounts. .	https://bitsight.com/
ProcessUnity	Offers automated third-party onboarding, tracks access entitlements, and manages lifecycle changes in identities to reduce over-priviliged access. .	https://processunity.com
Archer	Maps third-party SLA(Service Level Agreement) to identity privileges and quantifies risks tied to third-party account access and usage patterns.	https://archerirm.com
SecurityScorecard	Monitors third-party identity attack vectors in real time, including leaked credentials and misconfigured endpoints.	https://securityscorecard.com/
LogicGate	Agile GRC (Governance, Risk, and Compliance) cloud solution which builds automated workflows to review and manage vendor account permissions, helping align third-party identity practices with enterprise policies.	https://logicgate.com/
NAVEX Global	Manages the lifecycle of vendor identities, enforcing role-based access controls and helping validate compliance with identity governance standards.	https://navexglobal.com/
Panorays	Automates third-party security management, ensuring compliance with GDPR (General Data Protection Regulation).	https://panorays.com/
Secureframe	All-in-one platform which automates identity control evidence collection from vendors for standards like SOC 2 and ISO 27001 [Int22], ensuring proper identity authentication and provisioning.	https://secureframe.com/
Centraleyes	Cyber GRC (Governance, Risk, and Compliance) platform integrating internal and third-party risk management with real-time threat intelligence.	https://centraleyes.com/
LogicManager	Provides customizable questionnaires and AI analysis specifically targeting how vendors manage their own user identities and access policies.	https://logicmanager.com/

Prevalent	Simplifies vendor risk management by automating assessments and continuous monitoring.	https://prevalent.net/
OneTrust	Maps identity data flow of third-party identities and enforces third-party identity governance, including consent, access levels, and data minimization.	https://onetrust.com/
RiskRecon	Provides continuous monitoring and detailed risk assessments for third-party vendors.	https://riskrecon.com/
Tugboat Logic	Simplifies audits of vendor identity security controls and automates compliance tracking for third-party privileged access accounts.	https://tugboatlogic.com/
UpGuard	assesses vendor third-party identity risks through external scans and security ratings, detecting misconfigurations and weaknesses in third-party access controls.	https://upguard.com/
Vanta	Automates third-party user access reviews and ensures that external users meet compliance benchmarks for identity verification and access provisioning.	https://vanta.com/
Securiti	Tracks identity interactions between internal systems and third parties, providing granular controls over third-party access to sensitive identity data.	https://securiti.ai/

Table 1: Tool vendors

2.6 Research Gap

Despite extensive research on IAM, RBAC, PAM, and newer models like SSI, there is still no comprehensive academic framework that specifically addresses how to govern third-party identities. Current studies lack:

- A governance model made for to third-party and external users
- Support for temporary, dynamic and externally managed access
- Architectures and standards for monitoring, reviewing, and revoking third-party access

Although current solutions mainly address internal identities, the rapid growth of external users has introduced new and significant security risks. Industry reports from IBM, CyberArk, and SailPoint confirm that third-party identities are a major source of security breaches, often due to excessive access rights and poor account lifecycle management.
The literature shows that IAM systems have evolved to manage internal identities effectively, but the governance of third-party identities remains underexplored. Existing approaches lack the flexibility, automation, and oversight needed to handle today's external identity landscape. This gap highlights the need for a new framework designed specifically for third-party identity governance one that supports dynamic access, continuous monitoring, and automated lifecycle controls.

3 Case Studies of Third-Party Identity Governance Failures

The risks associated with third-party identity mismanagement are not theoretical, instead they have led to real-world security breaches that have caused financial losses, data leaks, and reputational damage. This chapter examines notable cybersecurity incidents that resulted from inadequate third-party identity governance. Each case is analysed to determine the root causes of the failure, and from these cases, we extract the essential requirements for an effective third-party identity governance framework.

Case 1. Okta Breach via Third-Party Support Engineer (2023)
In March 2023, Okta, a leading identity and access management (IAM) company, suffered a security breach due to a compromised third-party support engineers' credentials. Attackers gained unauthorised access to Okta's internal systems through an account that had excessive permissions. The third-party engineer had unnecessary permissions, allowing attackers to move laterally within Okta's environment, which means he had an overprivileged account. Also, there was a clear lack of continuous monitoring. Suspicious activities were not detected in time, allowing attackers to access sensitive data for even weeks. Unfortunately, this led to a delayed response since Okta initially underestimated the breach, leading to a slow containment of the attack. Key takeaways for the Third-Party Identity Governance (TPIG) include a Role-Based Access Controls (RBAC) in which external users should only have access to the minimal resources required for their tasks. Moreover, continuous monitoring and real-time alerts should be applied where suspicious activities from third-party accounts must be detected immediately. Furthermore, automated deactivation must be implemented in which third-party accounts should expire automatically after their required use period. [Cyb23]

Case 2. MOVEit File Transfer Breach (2023)
In May 2023, attackers exploited a vulnerability in MOVEit [ver24], which is a file transfer service. As a result of the attack, numerous organizations were impacted globally, including airlines, banks, and government agencies. The breach led to data leaks affecting millions of individuals, with estimated damages of 100 million dollars. One of the underlying issues were weak authentication controls. Many organizations using MOVEit failed to enforce multi-factor authentication (MFA) for third-party identities. Additionally, vulnerabilities in the software were not promptly addressed, leaving systems exposed. Similarly to the previous case, there was a unmonitored third-party access. Organizations did not adequately monitor third-party activities within the MOVEit system.
Focusing on breaking down key elements regarding TPIG from this case, it is important to implement a zero trust security model in which third-party identities should be authenticated and authorized continuously. Another aspect includes automated compliance audits in where organizations must ensure third-party tools meeting security patching and compliance requirements. Lastly, third-party accounts should have restricted access to critical systems which falls under privileged access management.

Case 3. ABN AMRO Data Breach via Third-Party Service Provider (2024)
In 2024, ABN AMRO disclosed a data breach caused by a ransomware attack on its third-party service provider, AddComm [Bey]. Sensitive client information was leaked due to inadequate security controls within the vendors' environment. In this case, ABN AMRO did not perform regular security audits of its third-party vendors. Similarly to the previous cases, third-party providers had excessive permissions, thus overprivileged access, and there was a slow response to this incident which led to significant data loss. ABN AMRO had shared sensitive client data with AddComm as part of their outsourced service delivery. Although ABN AMRO's internal systems remained unaffected, the breach within AddComm's environment led to the unauthorized exposure of that data. This underscores a key weakness in third-party identity governance: organizations must not only control internal access, but also ensure that external partners with access to sensitive data meet strict security standards.
From this case, it is important to consider risk management where organizations should perform regular security audits of third-party provider access. Another aspect of risk management includes access restrictions where external service providers should have the least amount of access. In order to respond adequately to this type of incidents from an organisational level, incident response planning should be implemented where predefined protocols are applied. This incident highlights the importance of implementing comprehensive third-party identity governance frameworks to mitigate risks associated with external partnerships as well.

Case 4: Microsoft SharePoint Mystery Users Incident (2023)
In a large Dutch enterprise using Microsoft SharePoint, employees noticed mystery users who had access to sensitive documents and shared resources. These accounts were leftover third-party identities that had not been deactivated after the users' contracts ended. In this specific case, there were third-party identities which remained active, long after they were no longer needed, also known as 'floating accounts'. Since there was no centralized system to track which third-party users had access, visibility was also lacking. From a policy level, the company had no logs to identify who granted access and when, meaning there were no audit trails. In order to prevent unauthorized users from accessing sensitive documents, and to maintain security, compliance, and effective access control, TPIG should be implemented. From a TPIG perspective, a form of a centralized identity governance is important assuring organizations to have a single system managing third-party identities and to do regular audits conducting routine reviews along with measurements mentioned in the previous 3 cases. This case is based on an incident that was personally observed during consultancy work, which means this is anecdotal evidence.

Problem	Description	Examples
Overprivileged Access	Third-party users have more access than necessary.	Okta, ABN Amro
Floating Accounts	Accounts remain active long after they should be deactivated.	Microsoft SharePoint, Okta
Weak Authentication	Third-party accounts lack strong security measures like MFA.	MOVEit
Lack of Visibility	Organizations cannot track what third-party users can access.	Microsoft SharePoint, ABN Amro
Slow Incident Response	Security breaches take too long to detect and mitigate.	ABN Amro, MOVEit, Okta

Table 2: Common Patterns in Third-Party Identity Failures

As shown in Table 2, examining these cases reveals recurring problems in third-party identity governance. These insights form the foundation for the governance framework proposed in this thesis

3.1 Summary of Key Takeaways

From these cases, it is evident that organizations need to adopt a structured approach to third-party identity governance. This includes:

1. **Role-Based Access Controls (RBAC):** Grant external users only the permissions they need. This solution mitigates the issue of overprivileged access by enforcing least privilege.

2. **Automated Lifecycle Management:** Ensure accounts are automatically deactivated when no longer needed, preventing floating accounts by promptly removing access when a third-party identity's engagement ends.

3. **Continuous Monitoring:** Implement real-time oversight of third-party accounts. With continuous monitoring, weak authentication and its related risks can be managed by detecting suspicious activity early, as weakly authenticated accounts require closer attention.

4. **Zero Trust Security Model:** Always verify who is accessing what and when.

5. **Vendor Security Audits:** Regularly assess third-party security postures before granting access. These audits help fix slow incident response by making sure partners have strong security and response plans, reducing the chances and impact of breaches.

The following chapters will discuss how these requirements can be integrated into an effective governance framework that organizations can implement to mitigate the risks of third-party identity mismanagement.

4 Governance Framework Design

4.1 Research Approach and Methodology

Managing third-party identities is an essential aspect of modern cybersecurity practices, as organizations increasingly depend on external collaborators to perform critical tasks. However, this reliance introduces significant risks, including floating accounts, overprivileged access, and insufficient monitoring.
This chapter outlines the methodology used to develop a governance framework specifically tailored to third-party identity management. The approach includes:

1. **Industry Review**
   Industry reports, and white papers on IAM systems and third-party identity governance were reviewed to identify gaps and limitations as described in Chapter 2. Special attention was given to works published in the last five years to ensure relevance.

2. **Tool Analysis**
   Commercial tools for third-party identity management were analyzed using a structured framework. This involved consulting industry experts, reviewing market research reports, and assessing tools based on criteria such as scope, integration capabilities, and focus on lifecycle management.

3. **Case Study Analysis**
   Real-life case studies of organizations managing third-party identities were examined to identify common vulnerabilities and challenges, such as floating accounts and overprivileged access as described in Chapter 3.

4. **Framework Synthesis**
   Findings from the literature, tool analysis, and case studies were combined to develop a structured governance framework tailored to third-party identities, which will be shown in Figures 4 and 5 of this chapter.

4.2 Application of the Data Governance Institute (DGI) Framework

4.2.1 Theoretical Foundation

The Data Governance Institute (DGI) framework [Ins24] is a widely recognized methodology for managing data governance. It emphasizes structured approaches to ensure data quality, security, and compliance, making it adaptable to address challenges in third-party identity governance. The key components of the DGI framework include:

- Mission and Value: Establishing strategic goals to protect sensitive information and ensure regulatory compliance.
- Governance Structure: Defining roles and responsibilities to manage external identities effectively.
- Data Quality and Stewardship: Implementing processes to maintain the integrity and accuracy of third-party account information.

- Policy and Compliance: Developing policies that align third-party governance with organizational standards and regulatory requirements.

While originally designed for data governance, this framework provides a solid foundation for addressing third-party identity management challenges. By modifying its components, organizations can create tailored solutions to manage external identities effectively.

By leveraging the DGI framework, organizations can systematically address the governance needs of third-party identities, ensuring that external access aligns with internal security policies and regulatory requirements .

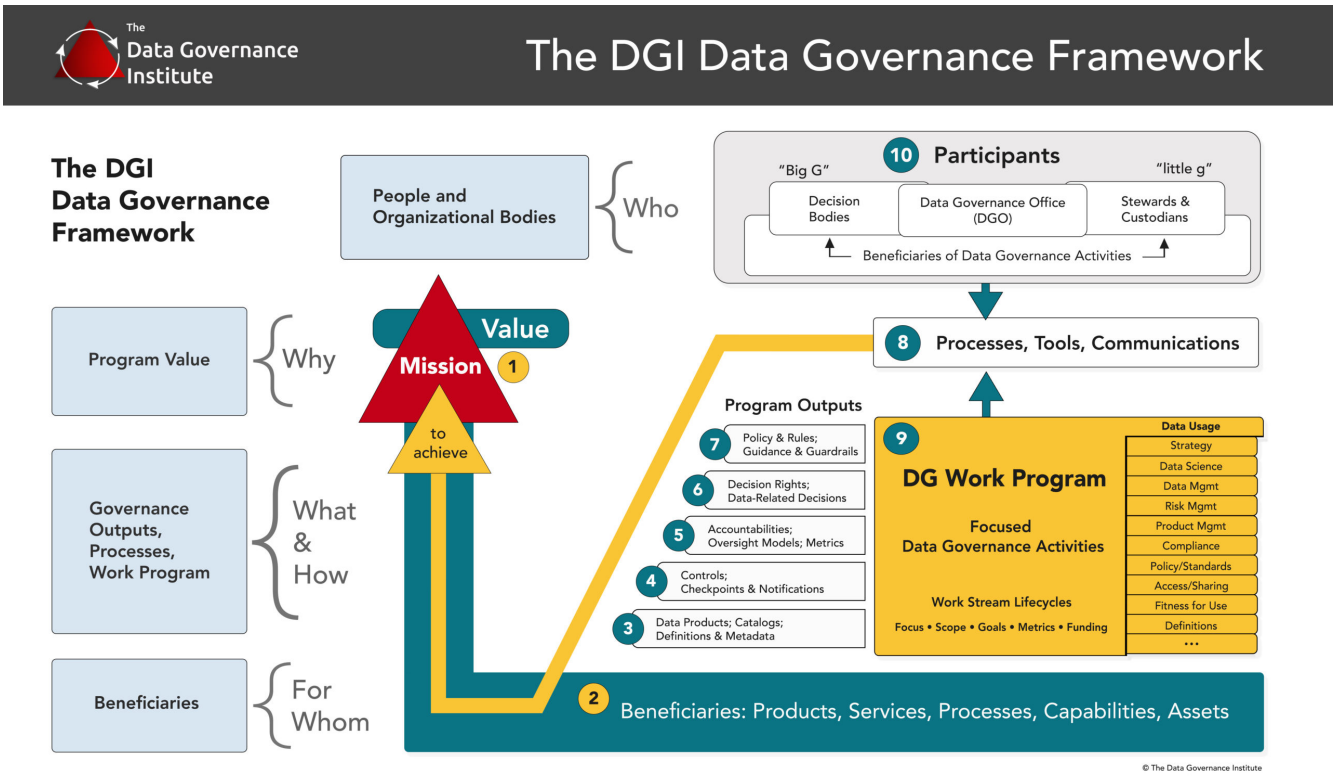

Figure 3. DGI Framework [Ins24]

4.2.2 Modifications for Third-Party Identity Management

A custom adaptation of the DGI framework has been developed to address the unique challenges posed by third-party identities. To support effective governance of third-party identities, we introduce the following modifications:

- Categorization of External Entities:
  - Entities are classified based on engagement type, access scope, duration, and compliance level.

  For example:

        * Engagement Type: Strategic partners, vendors, consultants.
        * Access Scope: Core systems or specific datasets.

- Trust and Risk Profiles:
    - Based on categorization, each entity is assigned a trust and risk profile. This determines the level of access and monitoring required.

- Customized Account Types and Management Strategies:
    - Accounts are tailored to the specific needs of each external collaborator, including:
        * Strategic Collaborator Accounts: Comprehensive lifecycle management for long-term partners.
        * Operational Contributor Accounts: Secure access with multi-factor authentication.

These modifications ensure that third-party accounts are governed with the same rigor as internal accounts, while addressing their dynamic and temporary nature.

Categorization

Category	**Description**	**Examples**
Engagement Type	Classify external entities based on the nature of interaction.	Strategic Partner, Vendor, Consultant
Access Scope	Define the breadth of systems, data, and resources the external entity requires access to.	Core Systems Access, Specific Data Sets Access
Engagement Duration	Distinguish between short-term projects, long-term partnerships, and intermittent access needs.	Short-Term Project, Long-Term Partnership, Intermittent Access
Security Compliance Level	Evaluate the external entity's adherence to recognized security standards and practices.	ISO 27001 Compliance [Int22], GDPR Compliance [Eur16]

Table 3: Categorization Framework for External Entities

Trust and Risk Profiles

Access Profile	Description
Strategic Access Profile	Low Risk, High Trust: For entities with proven security compliance and strategic importance to the organization, such as a long-term technology partner.
Operational Access Profile	Moderate Risk, Moderate Trust: For entities engaged in operational functions with access to non-critical systems, like a payroll processing vendor.
Project Access Profile	Variable Risk, Custom Trust: For entities requiring access for specific projects, with risk assessed based on sensitivity. For example, a contractor working on a sensitive data analysis project.
Restricted Access Profile	High Risk, Controlled Trust: For new or unverified entities requiring strict access controls and monitoring, such as a new supplier with minimal security history.

Table 4: Access Profiles and Descriptions

4.2.3 Implementation Strategy

The practical application of the modified DGI framework involves the following steps:

1. **Development of a Robust Categorization Framework:** Classify external entities based on their engagement type, access scope, duration, and security compliance level. This initial step tailors access management strategies to the specific needs and risks associated with each entity.

2. **Assignment of Trust and Risk Profiles:** Evaluate each entity against predefined criteria to assign them to the appropriate risk and trust profile. This assessment should be dynamic, allowing for reevaluation as engagements evolve or as new information becomes available.

3. **Tailoring Account Types and Management Strategies:** Determine the most suitable account types and management strategies for each external entity, including considerations for access scope, monitoring requirements, and compliance obligations. Implement the following:

- **Strategic Collaborator Accounts:** Use Identity Governance and Administration (IGA) [BG21] tools for comprehensive lifecycle management, ensuring ongoing compliance and security alignment. IGA tools help manage user identities and access permissions across systems.
- **Operational Contributor Accounts:** Secure access using Access Management (AM) solutions with Multi-factor Authentication (MFA) [WC21] and Cloud Access Security Brokers (CASB) for enhanced visibility and control over cloud interactions. AM solutions ensure

users authenticate securely, while CASBs protect cloud-based resources by enforcing security policies [FYW15].

- **Project Participant Accounts:** Employ Privileged Access Management (PAM) for granular control, using dynamic access policies to adapt to project phases and associated risks. PAM tools restrict access to critical systems, ensuring only authorized users have privileged access [Koo24].
- **Conditional Access Accounts:** Enforce strict conditional access policies for higher-risk entities, utilizing PAM for rigorous oversight and continuous monitoring solutions to detect and respond to anomalous behaviors promptly.

4. **Implementing Continuous Monitoring and Review:** Regularly review and update governance frameworks, tools, and strategies to adapt to new threats, technological advancements, and changes in the external entity landscape. This iterative process ensures the organization's approach to external identity and access management remains effective, compliant, and aligned with both operational needs and security objectives.
By implementing these modifications, organizations can effectively manage third-party identities, ensuring that external access is granted in a controlled manner that aligns with organizational security policies and compliance requirements.

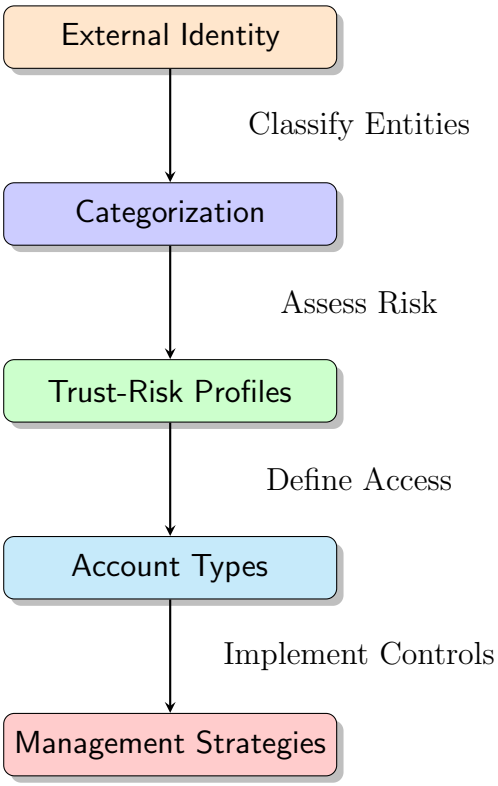

Figure 4: *C*lassify-*A*ssess-*D*efine-*I*mplement(CADI) Framework for External Identity Governance

Explanation:

- **External Identity**: Represents the third-party users requiring access to organizational resources.
- **Categorization**: Involves classifying external entities based on engagement type, access scope, duration, and security compliance level.
- **Trust-Risk Profiles**: Assigns trust and risk profiles to entities, determining the level of access based on assessed risks.
- **Account Types**: Defines the types of accounts and corresponding access privileges for each profile.
- **Management Strategies**: Implements controls and strategies for managing external identities and access.

4.3 Integration of key Governance Measures

Effective third-party identity governance requires an integrated approach that minimizes security risks, enforces strict access policies, and ensures continuous monitoring. Building on the structured foundation of the modified DGI framework, the proposed governance model integrates five key components that address recurring vulnerabilities in third-party identity management by enforcing real-time monitoring, access restrictions, and adaptive authentication mechanisms.

1. **Role-Based Access Controls (RBAC)** Granting external users only the minimum necessary permissions to perform their work. This helps prevent overprivileged access by making sure that users only get the access they need [Man19].
2. **Automated Lifecycle Management** Automatically removes third-party accounts when no longer needed, preventing floating accounts by ensuring outdated ones are not left active [Clu25].
3. **Continuous Monitoring** Real-time monitoring of third-party activities and logins helps reduce risks from weak authentication by quickly spotting unusual behavior or credential misuse, and speeds up incident detection [Min].
4. **Zero Trust Security Model** Applying the *'Never Trust, Always Verify'* approach to every access request, Zero Trust improves visibility by requiring ongoing authentication and authorization, while logging and monitoring each third-party access [IDP24].
5. **Vendor Security Audits** Regular security assessments of third-party vendors ensure that they meet the organisation's standards before access is granted. These audits help prevent slow incident response by identifying weaknesses in their security and incident handling ahead of time [UpG].

These five components build upon DGI's structured governance principles by incorporating real-time enforcement mechanisms that address third-party identity risks at a technical, procedural, and operational level.
By combining these components, organizations can establish a proactive and adaptive identity governance framework that effectively mitigates third-party security risks.

4.3.1 Role-Based Access Controls (RBAC)

Why RBAC?
Role-Based Access Control is a fundamental access control mechanism [Man19]. RBAC limits users to only resources and operations which are essential to their role. In the context of third-party identities, implementing RBAC helps ensure that external users operate under the principle of least privilege, reducing the risk of overprivileged accounts. Overprivileged third-party access remains a major security risk. As previously mentioned, CyberArk (2024) found that 82% of third-party identities had excessive privileges [Cyb24]. The 2022 Okta breach exemplifies this, where attackers exploited a third-party support engineer's over privileged account to gain unauthorized access to other internal systems . Proper RBAC policies could have limited such exposure.
Third-Party Identity Governance by using RBAC

- **Defining Specific Roles:** Creating custom roles for third-party users that grant only the necessary permissions for their roles.
- **Implementing Least Privilege:** Ensuring that third-party accounts have the minimum access required. This is done to reduce potential attack surfaces.
- **Utilizing Temporary Access:** Assigning time-bound roles that automatically expire. These roles are in line with the temporary role that many third parties have.
- **Conducting Regular Reviews:** Regularly audit the roles and permissions to update access and remove unnecessary privileges.

Framework Implementation:

- **Before access:** Assign third-party users to pre-assigned roles which align with their responsibilities. This is done to ensure they receive only necessary permissions.
- **During access:** Monitoring activities of third-parties in order to ensure compliance with their assigned roles and adjusting permissions if tasks change.
- **After access:** Removal of roles and associated permissions immediately after completion of any engagement of third-parties. This is done to prevent lingering access.

4.3.2 Automated Lifecycle Management

Why Automated Lifecycle Management?
Automated Lifecycle Management causes the creation, modification and deactivation of third-party accounts when needed [Clu25]. This minimizes the risk of any form of unauthorized access. Organizations often face floating accounts, which are accounts remaining active after they're no

longer needed. This increases the risk of unauthorized access. Implementing automated processes addresses these vulnerabilities by managing the entire third-party identity lifecycle.

Third-Party Identity Governance by using Automated Lifecycle Management:

- **Contract-Based Expiration:** By contract end-dates, deactivation of third-party accounts are aligned.
- **Inactivity Monitoring:** Unused accounts for a certain period will be automatically flagged and deactivated.
- **Periodic reviews:** In order to confirming the necessity of existing third-party accounts, regular reviews will ensure if only required access persists by e.g. looking at last login date reports.
- **Immediate Deprovisioning:** When contracts end, automated workflows will revoke access directly.

Framework Implementation:

- **Before access:** By Integrate identity lifecycle with contract management, setting set expiration dates for third-party accounts.
- **During access:** Monitor activity, adjusting permissions as roles or projects change.
- **After access:** Automatically deactivate or delete accounts when the contract is completed or inactivity.

4.3.3 Continuous Monitoring

Why Continuous Monitoring?
Third-party accounts stay a potential threat if they are not continuously monitored, despite the utilization of strict control on access and fast deprovisioning [Min]. This is due to the fact that for early detection and mitigation of anomalies or unauthorized behavior, real-time supervision of authentication and activity logs are essential. This approach is proactive, which in turn improves visibility and makes incident response faster.

Third-Party Identity Governance by applying Continuous Monitoring:

- **Unified Logging:** when all third-party logs are centralized within a Security Information and Event Management (SIEM) system [Sea], clearer visibility and facilitation of immediate threat detection and response will be provided.
- **Anomaly Detection:** using machine learning models to identify deviations from normal behavior on the accounts, such as unusual access times or unusual data transfer volumes.
- **SOC :** Ensuring that a Security Operations Center (SOC) [Exand] or Managed Security Service Provider (MSSP) continuously monitor and alert, which can initiate immediate responses.

- **Incident Response strategies:** in order to enable fasst and effective response, response strategies for various third-party account incident scenarios should be developed.

Framework implementation:

- **Before access:** Third-party users must undergo approval of access and identity verification.
- **During access:** In order to track anomalies, all actions are logged, monitored, and analyzed.
- **After access:** In order to prevent floating credentials, idle accounts will be automatically deactivated.

4.3.4 Zero Trust

Why Zero Trust?
The Zero Trust model [IDP24] is a cybersecurity approach that operates on the principle of *"Never Trust, Always Verify"*. Unlike traditional security models that assume users within the network are trustworthy, Zero Trust requires continuous authentication and strict access verification for all users, including third parties [Ano25].
Zero Trust Applies to Third-Party Identity Governance by Multi-Factor Authentication (MFA) in which All third-party accounts must use MFA to ensure strong authentication. Secondly, "least privilege access" is applied. Third-party identities only receive the minimum necessary permissions for their tasks. Last but not least, Session-Based Access Controls is applied, in which Access is granted on a temporary, session-based model rather than indefinite account privileges. Lastly, Real-Time Access Reviews should be incorporated. Continuous validation of third-party access, with automated expiration and renewal processes will minimize the risks. For example, in the MOVEit breach, attackers exploited weak authentication. If Zero Trust principles had been in place, MFA and continuous session validation could have blocked unauthorized access [ver24].

Third-Party Identity Governance by using Zero Trust:

- **Identity Verification (MFA):** All third-party accounts must authenticate using multi-factor authentication for every login session. Since only a username and a password are not sufficient, additional factors are required to verify the identity of the users [Sch19].
- **Least Privilege Enforcement:** All third-party users start with zero access and are only granted the specific required privileges.
- **Session Based Access Control:** Third-party access is only granted per session, and not through permanent logins. Additionally, sessions expire automatically after short periods of inactivity and re-authentication will be required. Access will be controlled by a Time-to-Live (TTL) which expires automatically after a set time.

Framework Implementation:

- **Before access is granted:** Third-party users must undergo identity verification and access approval.
- **During access:** Every action will be subjected to policy checks. For example, when a sensitive record is approached for access, an additional authorization step will be triggered. As a part of the continuous monitoring strategy, all activities will be logged and analyzed immediately.
- **After access:** Any tokens or issued temporary credentials will be revoked or expired. If the third-party needs access again later, they must start a new session with full verification.

4.3.5 Vendor Security Audits

Why Vendor Security Audits?
Vendor security audits are essential for evaluating and confirming that third-party identities from vendors, suppliers, or partners have appropriate security controls in place before they're granted access to systems or any form of data [UpG]. High-profile breaches have shown that attackers frequently target smaller vendors to compromise larger networks. For example, in a major 2013 retail breach, hackers used stolen credentials from an HVAC vendor to gain access to the retailer's systems [Mit].
Vendor Security Audits Apply to Third-Party Identity Governance by:

- **Pre-Access Checks:** Before giving vendors access, organizations check their security by using questionnaires and sometimes doing site visits.
- **Security in Contracts:** Contracts must include rules regarding security, for example, requiring vendors to use multi-factor authentication (MFA) and the obligation to report any security breaches.
- **Access Based on Security Level:**Vendors with strong security can get more access, while others may get limited access or need to improve their security first.

Framework Implementation:

- **Before access:** Set up a process to check risks by reviewing vendor security practices, policies, and certifications.
- **During access:** Keep track of vendor activities with regular checks and real-time monitoring to make sure they follow the agreed security rules.
- **After access:** When the contract ends or if there is a risk, all vendor access will be removed directly. Afterward, a review will be applied in order to understand how identity security has been managed.

Component	Purpose	Implementation in Third-Party Identity Governance
Zero Trust	Ensures that no access is granted by default and enforces continuous verification	MFA, least privilege access, real-time access reviews
Role-Based Access Control (RBAC)	Assigns access rights based on roles to ensure users have only necessary permissions	Define roles for third parties, implement least privilege, regularly review role assignments
Automated Lifecycle Management	Automates the provisioning and deprovisioning of accounts to reduce risk	Account expiration dates, automated deactivation, periodic access reviews
Continuous Monitoring	Provides real-time oversight to detect and respond to suspicious activities	24/7 threat monitoring, anomaly detection, automated responses

Table 5: Key Components in Third-Party Identity Governance

As a result, the proposed framework for implementation is shown in Figure 5.

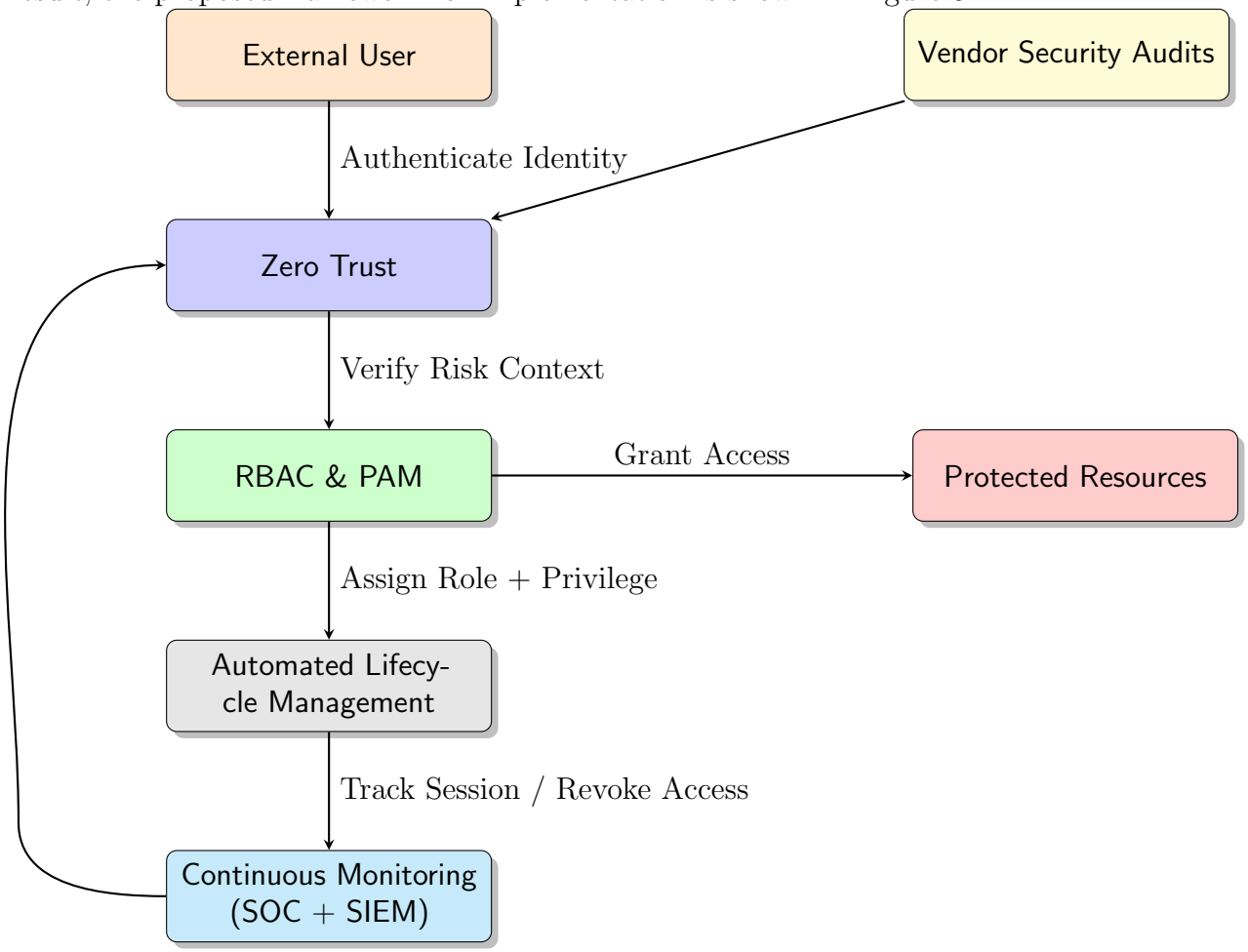

Figure 5: Governance-Based Architecture for Third-Party Identity Management

Integrated Workflow of the Governance Framework

1. **A third-party accounts requests access** → Verified through Zero Trust
2. **RBAC assigns minimal required access** → PAM enforces just-in-time elevation and session controls if needed.
3. **Lifecycle rules** → Accounts auto-expire, and changes in role/project update permissions.
4. **All sessions are monitored continuously** → SOC and SIEM systems log, alert, and respond to any anomalies.
5. **Vendor access is subject to security audits** → Non-compliant vendors may lose access or get restrictions.

4.4 Conclusion

This chapter outlined the methodology used to address the challenges of third-party identity governance. It presented a modified DGI framework and introduced a conceptual architecture by integrating five critical controls: Role-Based Access Control (RBAC), Automated Lifecycle Management, Continuous Monitoring, Zero Trust and Vendor Security Audits. These controls work simultaneously in order to address specific risk areas. These include overprivileged access, inactive accounts, weak authentication, limited visibility, and delayed incident response. The next chapter evaluates the effectiveness of the governance framework, it will also provide recommendations for its implementation across various industries.

5 Evaluation of the Governance Model

5.1 Overview

This chapter presents the findings of the study by analyzing how third-party identity governance affects cybersecurity risks. Additionally, the proposed governance framework from the previous chapter will be applied in a theoretical context to assess its impact. The results are based on case study evaluations, industry data, and governance model assessments. The aim of this Section is to validate the need for a structured governance framework by examining how well it addresses the security vulnerabilities identified earlier.

5.2 Scope of Risks regarding Third-Party Identity Vulnerabilities

5.2.1 Floating Accounts and Delayed Deprovisioning

- 41% of organizations struggle with identity governance maturity, leading to delays in deactivating third-party accounts [Tec24].
- **Case Study Findings:**
  - In the SharePoint environment of a Dutch enterprise, several public groups remained accessible to former contractors, exposing confidential documents.
  - In the Okta breach, a third-party support engineer's credentials were not deactivated after contract termination, leading to unauthorized access.
- **Impact Assessment:**
  - **Quantitative Data:** The 2024 IBM report found that floating accounts contribute to an average breach cost of $4.88 million.
  - **Solution Impact:** Automating deprovisioning can significantly reduce attack vectors, enhancing overall security posture [Gra25].

5.2.2 Overprivileged Access and Lateral Movement Risks

- In a study analyzing over 1,300 AWS accounts, researchers found that 82% of organizations granted third-party vendors highly privileged roles, leading to potential security risks and data exposure. [Tam21]
- **Case Study Findings:**
  - The ABN Amro breach involved a third-party vendor with excessive access to client data, which attackers exploited during a ransomware attack.
  - In the MOVEit breach, third-party access to file transfer services lacked strict access controls, facilitating data exfiltration.

- **Impact Assessment:**
  - **Quantitative Data:** 47% of organizations faced a data breach or cyberattack in the past year due to third-party access, with 34% linked to excessive privileged access [II25]. This highlights the security risk of overprivileged third-party identities
  - **Solution Impact:** Implementing Role-Based Access Control (RBAC) and Just-in-Time (JIT) access could reduce overprivileged accounts. NIST promotes Role-Based Access Control (RBAC) and Just-in-Time (JIT) access to stop unnecessary privileges. [Nat18]

5.2.3 Weak Authentication and Credential Management Failures

- Weak authentication practices are a major vulnerability for third-party accounts. Research from Verizon indicates that approximately 80% of data breaches stem from attackers gaining access via stolen or guessed credentials, exploiting weak passwords or single-factor logins [Ste23].
- **Case Study Findings:**
  - Attackers exploited an inactive VPN account belonging to a contractor of Colonial Pipeline. The account had no MFA and a weak password, allowing a ransomware group to access the network using only stolen credentials [Mic21].
  - In 2022, Uber was breached through a contractor's account. After obtaining the password, attackers launched an MFA brute attack; sending repeated push notifications until the user accidentally approved one [Vij22].
- **Impact Assessment:**
  - **Quantitative Data:** Verizon reports that most hacking-related incidents involve compromised passwords. Industry data shows that 99.9% of hijacked accounts lacked MFA [Sch19].
  - **Solution Impact:** Enforcing MFA, especially using strong factors like authenticator apps or hardware tokens, can block up to 99% of credential-based attacks. Microsoft found that MFA-enabled accounts are 99.9% less likely to be compromised.

5.2.4 Lack of Continuous Monitoring and Incident Response Gaps

- 292 days on average to detect and contain a breach caused by third-party credentials [IBM24].
- **Case Study Findings:**
  - The Okta breach was undetected for weeks, allowing attackers extended access to internal systems. Third-party access was not continuously monitored, enabling persistent threat infiltration.
- **Impact Assessment:**
  - **Quantitative Data:** Organizations with Security Operations Centers (SOC) and real-time monitoring detect breaches 40% faster [Cor23].

- **Solution Impact:** Implementing Security Operations Center (SOC) with real-time monitoring significantly reduces the time to detect and contain security incidents. Continuous monitoring enables early identification of threats, thereby minimizing potential damage and facilitating swift restoration of normal operations [Sec25a].

5.2.5 Slow Incident Response

- Unfortunately, many organizations follow with slow incident responses after a third-party related breach is discovered. Delays in containment and remediation give attackers more time to inflict harm or steal data. According to IBM data, organizations take an average of 73 days to contain a breach after detecting it. When a third-party is involved, incident response can be even more complicated and sluggish, as seen by the fact that supply chain breaches in 2023 took 12.8% longer to contain than breaches with no third-party involvement [Bon25].
- **Case Study Findings:**
  - In the breach ABN Amro/AddComm in 2024, ABN Amro was unfortunately depended on its vendor to investigate and report the incident. Nevertheless, AddComm eventually contained the ransomware, the slow incident report limited ABN Amro's ability to act immediately by, for example, alerting clients and/or disabling affected systems.
  - The 2022 Okta support engineer breach highlighted slow incident response. Public disclosure was delayed by nearly two months due to extended analysis and coordination with the contractor. This left customers at risk and drew criticism from experts and regulators for the delayed communication [Sha22].
- **Impact Assessment:**
  - **Quantitative Data:** IBM found that breaches contained within 30 days cost over $1 million less than those that took longer. [IBM24]
  - **Solution Impact:** Immediate and coordinated response which includes real-time monitoring, automated scenario workflows and strong collaboration with vendors.

5.3 Performance of the Proposed Governance Framework

This Section assesses how well each component of the proposed governance framework from Chapter 4 addresses the third-party risks identified above. The goal is to assess how well the five governance measures reduce key risks: floating accounts, overprivileged access, weak authentication, limited visibility, and slow incident response.

5.3.1 Zero Trust Impact on Authentication and Access Control

- **Findings from Industry Reports:**
  - A report from IT Brew in February 2023 highlighted that only 28% of Microsoft users had enabled Multi-Factor Authentication (MFA) as of December 2022. This low adoption rate indicates that third-party identities are particularly vulnerable to unauthorized access attempts [Hig23].

    * Forrester Research emphasizes that adopting a Zero Trust security framework can significantly enhance an organization's security posture. By limiting partner access, protecting data with encryption, and segmenting networks, organizations can reduce the risk of data breaches and privacy abuses associated with access through third-party accounts [For23].
  - **Key Takeaway:** Unauthorized access attempts will be reduced by strengthening MFA enforcement and real-time access validation throug Zero Trust.

5.3.2 Role-Based Access Control (RBAC) for limiting excessive privileges

  - **Findings from Industry Reports:**
    * The 2024 Identity Security Threat Landscape Report indicates that compromised privileged identities accounted for 33% of security incidents, up from 28% in 2023. [Bey24]
    * According to the Ponemon Institute's 2022 report, 51% of respondents stated that managing and securing third-party remote access is becoming increasingly difficult due to lack of centralized access control and visibility. These key challenges that RBAC is designed to address [Pon22].
  - **Key Takeaway:** Implementing RBAC combined Just-in-Time access reduces the risk of overprivileged third-party identities. This is done by assigning external users minimal roles and allowing temporary access only when needed, organizations reduce the risk of privilege misuse and limit cross system movement.

5.3.3 Automated Lifecycle Management

  - **Findings from Industry Reports:**
    * Omada Identity explains that if access isn't removed when someone leaves, orphaned accounts can be left behind and may be misused. Automated lifecycle management, as part of Identity Governance and Administration (IGA), helps make sure access is removed on time, reducing security risks [Oma24].
    * CloudEagle.ai illustrates that slow removal of access is a common problem that can lead to insider threats and compliance issues, especially during merging between organizations. Automating identity lifecycle processes helps reduce these risks by making sure access is removed quickly and consistently [Shr25].
  - **Key Takeaway:** Automating the lifecycle of third-party identities helps avoid active access after offboarding, which in turn reduces the risks.

5.3.4 Continuous Monitoring

  - **Findings from Industry Reports:**
    * IBM reports that third-party breaches take 292 days to detect without continuous monitoring, but only 90 days with it.

    - Organizations with fully deployed security automation experience average data breach costs of 3.15 million dollars, while those without face costs of 6.71 million dollars [IBM24].
  - **Key Takeaway:** Continuous monitoring enables faster threat response through real-time alerts and anomaly detection.

5.3.5 Vendor Security Audits

  - **Findings from Industry Reports:**
    - SecurityScorecard Global Third-Party Breach Report revealed that 35.5% of all breaches in 2024 were third-party related, underscoring the significant risk posed by vendors and the necessity for rigorous security assessments [Sec25b]. Also, threat actors are increasingly leveraging supply chains as entry point, which highlights the need for organizations to move from periodic vendor audits to real-time monitoring.
  - **Key Takeaway:** Regular vendor audits and continuous monitoring help in accomplishing security standards by reducing breach risk and faster response times to incidents.

Identified Issue	**Quantitative Impact**	**Proposed Solution & Improvement**
Floating Accounts	$4.88 million average breach cost when orphaned accounts are involved [IBM24]	Automated deprovisioning ensures timely removal of access, reducing the risk of misuse [Gra25]
Overprivileged Access	34% of breaches linked to excessive third-party privileges [II25]	Implementing RBAC with Just-in-Time access limits privileges, reducing misuse risk [Nat18]
Weak Authentication	80% of breaches involve weak or stolen credentials [Ste23]	Enforcing MFA within a Zero Trust framework significantly reduces unauthorized access attempts [For23]
Limited Visibility	292 days on average to detect credential breaches [IBM24]	Continuous monitoring reduces detection time to approximately 90 days, enabling faster response [Cor23]
Slow Incident Response	73 days average to contain a breach after discovery [IBM24]	Regular vendor audits and continuous monitoring ensure third parties meet security standards, improving response times [Sec25b]

Table 6: Alignment of key third-party risks with governance solutions and their impact

5.4 Conclusion

The findings confirm that a governance model built on Zero Trust, RBAC, automated lifecycle management, continuous monitoring and vendor audits help reducing risks associated with third-party identities. Each component addresses vulnerabilities which include orphaned accounts, overprivileged access, weak authentication, limited visibility, and slow incident response. Real-time monitoring and automated processes will shorten exposure windows, while strict access controls and vendor oversight will limit potential attack surfaces and contain threats more effectively. Based on these findings, these controls could lead to fewer security incidents, faster detection, containment of the incident and also breach-related costs. Also, an automated system approach to third-party identity governance is highlighted.

6 Implementation and Future Considerations

6.1 Framework Status and Implementation Readiness

The governance framework proposed in this thesis is currently a conceptual model designed to address the challenges of third-party identity management in order to improve security from a system view. The proposed framework uses principles from Identity and Access Management (IAM) systems and adapts them to external accounts, however it has not yet been implemented in a real-world organizational context. Also, further refinement and empirical testing are required to evaluate its effectiveness fully and adapt it in practice.

6.2 Preliminary Industry Feedback

Preliminary feedback on the proposed framework was obtained from a senior Identity and Access Management (IAM) consultant at SonicBee, a cybersecurity firm specializing in IAM health checks and governance roadmaps. The consultant had previously worked on an IAM project for a Dutch municipality, in which managing third-party identities such as contractors, cleaners, and security personnel was a major challenge. The difficulty in governing these external identities, despite the availability of various tools, resulted in the initial idea for the research question for this thesis.

A couple of months later, the consultant was contacted again to present a draft version of the proposed framework and request structured feedback. The feedback included the following components:

1. Modular Design: The practicality of the framework's modular components (e.g., lifecycle management, RBAC, and monitoring) got emphasized.

2. Automation and Monitoring: The integration of automation and continuous monitoring was highlighted as a core strength, offering solutions to common limitations in current IAM toolsets.

3. Regulatory Alignment: The framework's adherence to compliance standards, such as GDPR [Eur16] got recognized as a valuable aspect, ensuring alignment with both legal and operational requirements.

While this expert feedback affirms the relevance and practicality of the framework, it also reinforces the importance of further testing and refinement to ensure scalability and real-world applicability across diverse organizational environments.

To transition the proposed framework from a conceptual model to a practical solution. The following phases are a start to transition the proposed framework from a conceptual model to a practical solution.

1. **Collaborative Pilots:** Partner with organizations across industries to implement the framework in controlled environments. These pilots will highlight operational challenges and identify areas for improvement.
2. **Iterative Testing and Feedback Loops:** Develop iterative versions of the framework based on pilot outcomes. Each iteration will incorporate feedback to address identified gaps.

The initial feedback illustrated that the framework is easy to implement. Also, it's aligned with IAM practices and it includes automation and monitoring which were major sources of potential risks as described earlier. Nevertheless, the framework requires validation with pilot implementations, iterative development, and formal empirical studies.

The next chapter summarizes the research contributions and identifies opportunities for future work.

7 Conclusion

7.1 Summary of Research Contributions

This thesis contributes to the field of identity governance by addressing critical gaps in existing IAM systems and proposing a governance framework focusing third-party identities. The key contributions include:

1. Identified Vulnerabilities:
   - Important risks associated with third-party identities are identified which include overprivileged access, floating accounts, weak authentication, lack of visibility, and slow incident response.
2. Proposal of a Conceptual Framework:
   - A governance framework was developed based on industry reports which addresses directly five major risks, with additional five corresponding security measures. These are role-based access controls (RBAC), automated lifecycle management, continuous monitoring, Zero Trust security principles, and vendor security audits. It builds upon established IAM and data governance concepts (such as the DGI framework).
3. Laying the Foundation for Future Work:
   - The framework is only an initial step toward developing standardized and validated solutions for third-party identity governance. Future research should focus on validating each component in the proposed architecture presented in this thesis. Also, monitoring the implementation stages of these systems and understand the impact of each component on the identified vulnerabilities.

7.2 Limitations of the Study

Although his research provides a strong foundation, several limitations must be achknowledged. First, the proposed framework remains theoretical based on objective findings, and has not yet been implemented and validated for real-work environments. Furthermore, the research focuses primarily on technical vulnerabilities (lifecycle management) and does not explore organizational challenges such as cultural resistance to adopt new governance frameworks, and thus does also not take socio-technical aspects into account. Lastly, the framework assumes integration within mature IAM platforms, which may be not available in all organizations so there is dependence on existing IAM systems. However, these limitations provide opportunities for future research and developments in order to strengthen the applicability and effectiveness of the proposed framework.

7.3 Directions for Future Research

Building on this research, future work should focus on:

1. **Pilot Testing** Pilot implementations and validation studies are needed to assess the frameworks' effectiveness in real-world scenarios.
2. **AI/ML Integration:** Exploring how artificial intelligence and machine learning can enhance monitoring and anomaly detection capabilities.
3. **Exploring Organizational Challenges:** Investigating cultural and operational barriers to adopting third-party identity governance frameworks.
4. **Developing Industry-Specific Variations:** Customizing the framework for sectors with unique requirements, such as critical infrastructure and regulated industries.

Third-party identity governance is an increasingly critical cybersecurity challenge, as organizations rely more on external collaborators. By addressing the unique vulnerabilities of third-party identities, this thesis contributes to closing an important gap in existing IAM practices. Although the proposed framework is conceptual, it provides a foundation for future research, development, and practical implementation.

As the reliance on external collaborators continues to grow, advancing third-party identity governance frameworks will remain essential for ensuring security, compliance, and operational efficiency.

In conclusion, this thesis examined the unique security challenges of third-party identities. It proposed a conceptual governance framework designed to mitigate key risks. By integrating technical controls and existing governance controls like Role-Based Access Control(RBAC), Automated Lifecycle Control, Zero Trust, continuous monitoring and vendor audits the framework lays the groundwork for structured third-party identity governance. While the framework is still conceptual, it shows the need for stronger identity management, as organizations work more with third-parties. The proposed governance model offers a starting point for future research, validation and practical implementation in the field of third-party identity management.

References

[Ano25] Anomalix. Third party identity and access governance, 2025. Available at https://www.anomalix.com/whitepapers/zero-trust-for-non-employee-third-party-individuals.

[Bey] Beyondidentity. Free Open Breaches Database - BreachHQ by Beyond Identity. Available at https://breach-hq.com/organizations/abn-amro.

[Bey24] BeyondTrust. The state of identity security for 2024: Identity-based threats, breaches, and security best practices, 2024. Available at https://www.beyondtrust.com/blog/entry/the-state-of-identity-security-identity-based-threats-breaches-security-best-practices.

[BG21] E. Bago and I. Glazer. Introduction to identity - part 1: Admin-time (v2). *IDPro Body of Knowledge*, 1(5), 2021.

[BMHR24] Paul Baumer, Sebastian Marczak, Asad Hussain, and Christian Reuter. Digital nudges for access reviews: Guiding deciders to revoke excessive authorizations. In *Proceedings of the 2024 Symposium on Usable Privacy and Security (SOUPS)*, 2024. Available at https://www.usenix.org/system/files/soups2024-baumer.pdf.

[Bon25] Emily Bonnie. 110+ of the latest data breach statistics [updated 2025], January 2025. Available at https://secureframe.com/blog/data-breach-statistics.

[BSZ23] Tianyi Shan Bingyu Shen and Yuanyuan Zhou. Improving logging to reduce permission over-granting mistakes. In *Proceedings of the 32nd USENIX Security Symposium*, 2023. Available at https://www.usenix.org/system/files/usenixsecurity23-shen-bingyu-logging.pdf.

[CG22] Andrew Cameron and Oliver Grewe. An overview of the digital identity lifecycle (v2). *IDPro Body of Knowledge*, 1(7), 2022.

[Clu25] Clutch Security. Understanding the Identity and Access Management (IAM) Lifecycle, 2025. Available at https://www.clutch.security/blog/iam-lifecycle/.

[Cor23] Microsoft Corporation. Microsoft digital defense report 2023. Technical report, 2023. Available at https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

[Cyb23] CyberArk. Piecing together the attack on okta's support unit, 2023. Available at https://www.cyberark.com/resources/blog/piecing-together-the-attack-on-oktas-support-unit.

[Cyb24] CyberArk. Identity security threat landscape 2024 report, 2024. Available at `https://www.cyberark.com/resources/ebooks/identity-security-threat-landscape-2024-report`.

[Eur16] European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). `https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679`, 2016.

[Exand] Exabeam. SIEM vs. SOC: 4 Key Differences and How They Work Together. https://www.exabeam.com/explainers/siem-security/siem-vs-soc-4-key-differences-and-how-they-work-together/, n.d. Available at https://www.exabeam.com/explainers/siem-security/siem-vs-soc-4-key-differences-and-how-they-work-together/.

[For23] Forrester. Zero trust security: The business benefits and advantages, 2023. Available at https://www.forrester.com/zero-trust/.

[FYW15] Eduardo B. Fernández, Nobukazu Yoshioka, and Hironori Washizaki. Cloud access security broker (casb): A pattern for accessing secure cloud services. In *Proceedings of the 4th Asian Conference on Pattern Languages of Programs (AsianPLoP 2015)*, March 2015. Available at https://www.researchgate.net/publication/272943367_Cloud_Access_Security_Broker_CASB_A_pattern_for_accessing_secure_cloud_services.

[Gra25] Kaitlyn Graham. Third-party data breach: Definition & 5 examples, January 2025. Available at https://www.bitsight.com/blog/third-party-data-breach.

[GSFF23] Jana Glöckler, Johannes Sedlmeir, Muriel Frank, and Gilbert Fridgen. A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity. *Business Information Systems Engineering*, 66(4):421–440, 9 2023.

[Hig23] Eoin Higgins. Lack of mfa adoption from microsoft users raises concerns over security, February 2023. Available at https://www.itbrew.com/stories/2023/02/17/lack-of-mfa-adoption-from-microsoft-users-raises-concerns-over-security.

[IBM24] IBM. Cost of a data breach report 2024, 2024. Available at https://www.ibm.com/reports/data-breach.

[IDP24] IDPro Team. The identity-driven reality of zero trust, July 2024. Available at https://idpro.org/the-identity-driven-reality-of-zero-trust/.

[II25] Ponemon Institute and Imprivata. Imprivata study finds nearly half of organizations suffered a third-party security incident in past year, February 2025. Available at https://www.globenewswire.com/news-release/2025/02/13/3025931/0/en/Imprivata-Study-Finds-Nearly-Half-of-Organizations-Suffered-a-Third-Party-Security-Incident-in-Past-Year.html.

[Ins24] Data Governance Institute. Dgi data governance framework, 2024. Available at https://datagovernance.com/the-dgi-data-governance-framework/.

[Int22] International Organization for Standardization. ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://www.iso.org/standard/27001, 2022.

[Koo24] A. Koot. Introduction to privileged access management. *IDPro Body of Knowledge*, 1(13), 2024.

[Man19] Sri Kanth Mandru. Role-based access control (rbac) in modern iam systems: A study on the effectiveness and challenges of rbac in managing access to resources in large organizations. 04 2019.

[McK21] Mary McKee. Policy-based access controls. *IDPro Body of Knowledge*, 2021. Available at https://bok.idpro.org/article/61/galley/78/view/.

[Mic21] Michael Novinson. Colonial pipeline hacked via inactive account without mfa, 2021. Available at https://www.crn.com/news/security/colonial-pipeline-hacked-via-inactive-account-without-mfa.

[Min] MindPoint Group. What is Continuous Monitoring and How Does it Work in a SOC? `https://www.mindpointgroup.com/blog/continuous-monitoring-soc`. Available at https://www.mindpointgroup.com/blog/continuous-monitoring-soc/.

[Mit] Mitratech Staff. The 2013 target data breach: A lasting lesson in third-party risk management. Available at https://mitratech.com/resource-hub/blog/the-2013-target-data-breach-a-lasting-lesson-in-third-party-risk-management/.

[Moh17] Ishaq Azhar Mohammed. Systematic review of identity access management in information security. *SSRN Electronic Journal*, 4:1–7, 07 2017.

[Nat18] National Institute of Standards and Technology. Framework for improving critical infrastructure cybersecurity, version 1.1. Technical report, U.S. Department of Commerce, April 2018. Available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[Oma24] Omada Identity. Why deprovisioning access is so important in cybersecurity, October 2024. Available at https://omadaidentity.com/resources/blog/importance-of-access-deprovisioning/.

[Pon22] Ponemon Institute. The state of cybersecurity and third-party remote access risk. Technical report, Ponemon Institute, 2022. Available at https://security.imprivata.com/rs/413-FZZ-310/images/SL-Ponemon-Report-state-of-cs-and-third-party-access-risk-1122.pdf.

[Sch19] Dan Schuyler. Microsoft: Using multi-factor authentication blocks 99.9% of account hacks, August 2019. Available at https://blog.vlcm.com/blog/multi-factor-authentication.

[Sea] SearchInform. Continuous Monitoring with SIEM: Tools and Techniques. `https://searchinform.com/cybersecurity/measures/siem/management/continuous-monitoring/`. Available at https://searchinform.com/cybersecurity/measures/siem/management/continuous-monitoring/.

[Sec25a] Radiant Security. Mastering soc incident response process: Strategy and key steps, February 2025. Available at https://radiantsecurity.ai/learn/soc-incident-response/.

[Sec25b] SecurityScorecard STRIKE Threat Intelligence Unit. 2025 global third-party cybersecurity breach report. Technical report, SecurityScorecard, March 2025. Available at https://securityscorecard.com/resource/global-third-party-breach-report/.

[Sha22] Ax Sharma. Okta: "we made a mistake" delaying the lapsus$ hack disclosure, March 2022. Available at https://www.bleepingcomputer.com/news/security/okta-we-made-a-mistake-delaying-the-lapsus-hack-disclosure/.

[Shr25] Madhu Shrinivas. Identity governance challenges during mergers and acquisitions: What cisos must know, May 2025. Available at https://www.cloudeagle.ai/blogs/identity-governance-challenges-during-mergers-and-acquisitions-what-cisos-must-know.

[Ste23] Stephanie Domas. Using third-party identity providers in a zero trust world, 2023. Available at https://www.darkreading.com/cyber-risk/using-third-party-id-providers-zero-trust.

[Tam21] Shir Tamari. Identity-based supply chain risk is new and serious, February 2021. Available at https://www.wiz.io/blog/82-of-companies-unknowingly-give-3rd-parties-access-to-all-their-cloud-data.

[Tec24] SailPoint Technologies. The horizons of identity security: Harnessing the power of identity security to bend the cybersecurity value curve, 2024. Available at https://docs.sailpoint.com/wp-content/uploads/SailPoint-Horizons-of-Identity-Security-Report-2024-2025-SP2487.pdf.

[UpG] UpGuard. ISO 27001 Third-Party Risk Requirements: What You Need to Know. Available at https://www.upguard.com/blog/iso-27001-third-party-risk-requirements.

[ver24] 2024 data breach investigations report. Technical report, Verizon, 2024. Available at https://www.verizon.com/business/resources/reports/dbir/2024/.

[Vij22] Jai Vijayan. Uber: Lapsus$ targeted external contractor with mfa bombing attack, September 2022. Available at https://www.darkreading.com/cyberattacks-data-breaches/uber-breach-external-contractor-mfa-bombing-attack.

[WC21] Joseph Williamson and Kevin Curran. Best practice in multi-factor authentication. *Semiconductor Science and Information Devices*, 3, 05 2021. 10.30564/ssid.v3i1.3152.

[XLJ23] Runhua Xu, Chao Li, and James Joshi. Blockchain-based transparency framework for privacy preserving third-party services. *IEEE Transactions on Dependable and Secure Computing*, 20(3):2302–2313, 2023.