PART 1: ENVIRONMENTAL DESCRIPTION

AcmeDataCorp is a medium-sized organization operating in the financial sector, handling highly sensitive information. The type of information in operation involves: customer personal and commercial data, internal financial documents, stock market and investment operations information, critical IT infrastructure. Due the nature of its business AcmeDataCorp (ADC) is exposed to high level of financial, regulatory, legal as well as reputational risk related to information security.

1. Roles and responsibilities

The organization uses the role-based structure revolving around the following groups:

- **Finance**: responsible for main operations, financial documents, stock market ops, reports
- **HR**: responsible for employee oversight, personnel management, contracts, personal data
- **IT-Admins**: responsible for IT infrastructure, operational and data security, system admin
- **Managers**: responsible for operations oversight and decision making
- **Interns**: temporary employees in training

2. Protected resources

- **Finance Docs**: highly confidential financial data revealing trading secrets, company fiscal reports, B2B operations, necessary client financial details, prognoses. Heart of the company's operations
- **Archive**: historical records, data required to keep legal reasons, backups
- **Top Secret IT**: extremely sensitive information regarding IT security and system information i.e.: encryption keys, root credentials, AD structure, API endpoints, VPN and firewall settings
- **Common**: shared workspace for collab across the company's employees with various privileges

3. Access Control at ADC is implemented through a layered authorization model combining RBAC, DACL and SACL enforcement.

- **RBAC (Role Based Access Control)** defines defines who is allowed to request access by assigning users to predefined business roles (Finance, HR, IT-Admins, Managers, Interns). These roles act as security principals and are mapped directly to permissions to access resources.
- **DACL (Discretionary Access Control List)** applied to each resource define what actions each role may perform (Read, Modify, Full Control), making the authorization deterministic and enforceable at the object level.
- **SACL (System Access Control List)** works in parallel with DACL and determines which access attempts are audited allowing tracing both successful and denied actions.
  This model allows administrators or resource owners assign permissions to their own discretion rather than rely on fixed security settings as in MAC (Mandatory Access Control, where access is enforced based on fixed classification). The pro of such system is that is allows granular control of individual access, the con is that it's more control-demanding in the way that slight errors in configurations lead directly to unauthorized access.
- **The Principle of Least Privilege** is a security model based on access only to bare minimum resources required for an employee to their job. Based on employee job description he or she will be only granted access to basic resources in order to fulfill their job duties. Risk arises in situations where a company, for various reasons from financial constraint, negligence, overwork or laziness offloads extra duties on employees beyond their job description. For instance junior admin may be required to do part of senior admin job or manager may have to do sales job which requires access to extra data and resources. Unfortunately these types of situations aren't uncommon in workplace and must be taken into consideration when analyzing security risks.

4. The authentication is based on:
- Password following minimal complexity policy
- MFA (Multi Factor Authentication) is enforced but only for admin users, which is not a strategic approach, considering that a finance company doesn't enforce stricter protection rules around its core operations and double-verify access by Finance staff.
- Logins are logged with success/failure

This presents very weak security posture, especially for non-admin users, which is only better than nothing but in reality largely inadequate to fully protect company's operations and assets.

5. The company has exposure to the following attacks:

SECURITY THREAT	EXAMPLE (some not all)
General (faced by every company, no matter security level)	- Malicious/vindictive employees looking to damage company's (or colleagues') assets or reputation - Delegating responsibilities to employees above their job description - Threats (not necessarily malicious) from third party actors involved in company's supply chain, in this case financial institutions, partners etc that when compromised themselves may put ADC, their employees and clients at risk.
Legal	- No strict protection around employee and customer data which, depending on the country ADC is based in, may be not compliant with national, federal or supranational data protection regulations (like GDPR) - Breach or leaking financial data can be linked to legal issues with global legislation and financial bodies
Structural	- The company doesn't have a strictly designed sales, escalation and customer service team which may not be required but in order for the operations to run someone has to do it. That means that this someone will have unlimited access to customer data beyond their current job description, without accountability. This is extreme risk.
Technical	- No MFA for Finance and HR access, weak password complexity = credential compromise - Indiscriminate access to the Common folder = data leakage - No geo-blocking, travel rules for remote access = account hijacking - Misconfigured, broad RBAC = privilege escalation
Financial	Managers can self-assign membership in Finance group which can lead to insider trading. Interns or a non-MFA account user can alter financial reports audits that can lead to stock manipulation. The fact that former HR member had active access and Financial documents aren't MFA protected can lead to asset and data theft.

PART 2. INCIDENT ANALYSIS

1. An Intern user mistakenly changed a financial file

WHAT HAPPENED: The Intern group had incorrectly granted rights on Finance documents and one of its member accidentally modified a financial report.
WHO/ROLE: An Intern user
ACCESS MODE: Modify
IAM PRINCIPLES BROKEN: Least Privilege, Separation of Duties, Need-to-Know, Regularly Audit Access to Resources
HOW IT HAPPENED: It happened due to RBAC design failure such as inherited permissions from parent group, unintentional group nesting or wide delegation rights resulting in excessive privileges. Interns should have only minimal access and only to files that concern them, meanwhile incorrect DACL privileges allowed them elevated access. In addition to that there was no oversight to spot the error.
POTENTIAL CONSEQUENCES:
- faulty financial data in circulation. Company's financial calculations based on incorrect numbers
- the possibility of tax/financial fraud if altered document processed unnoticed
- unwarranted insight into sensitive data. Even if accidental, the door is still open to for attackers to manipulate and steal financial assets or sabotage the company
- possible non compliance with individual data protection laws
- wider loss of trust in data security amongst employees and/or customers
LOG INFO: File access attempt (4663), Handle to object request (4656) → shows file modification.
WHY A PROBLEM: This incident shows weak privilege administration and governance during the lifecycle management as basic access policies were not enforced and not monitored.

2. Former HR employee logs in work account two weeks after terminating his position

WHAT HAPPENED: A former HR employee could log into his account two weeks after his last day at work due to faulty off-boarding procedure.
WHO/ROLE: A former HR employee
ACCESS MODE: Login
BROKEN IAM PRINCIPLES: Least Privilege, Zero Trust, Lifecycle Management, Audit Access
HOW IT HAPPENED: Failure in decommissioning an inactive account. The off-boarding procedures were either not enforced or not properly followed through. Since it's said that audit fails or is delayed, no one double checked if the closing procedure was successful.
POTENTIAL CONSEQUENCES
- industrial espionage
- social engineering
- asset or data theft
- non-compliance with data protection laws
- unwarranted access to personnel data
LOG INFO: Successful logon (4624), Failed logon (4625), check for Enabled user account (4722) → successful login from deactivated account. Also check for lack of (!) audit log upon closure.
WHY A PROBLEM: This is a process failure and a technical failure. It exposes vulnerability in lifecycle management enforcement and lack of oversight over faulty audit tools. A log (4725) confirming disabled account should have appeared upon removing the account

3. 72 failed login attempts overnight

WHAT HAPPENED: A Finance account had 72 failed login attempts over between 2.00-3.00am
WHO/ROLE: Finance
ACCESS MODE: Login & Authentication
BROKEN IAM PRINCIPLES: Secure Authentication- no MFA on Finance accounts, Prevention and Monitoring- no *fail2ban*-type blocking tools in place
HOW IT HAPPENED: As above- no MFA on Finance and weak sever protection against brute-force attacks or credential hijacking attempts.
POTENTIAL CONSEQUENCES:
- data breach and leak
- account compromise
- severe financial, legal and reputational consequences
- financial fraud
- asset theft
LOG INFO: Failed logon (4625), Kerberors auth failure (4771), Account locked (4740) if account gets locked after multiple failed login requests → look for multiple failed logins and time of access
WHY A PROBLEM: It shows weak authentication protection and conditional access enforcement, poor server protection possibly resulting in irreversible consequences to the company's operation and reputation

4. An IT admin logs from another country while on vacation

WHAT HAPPENED: An admin account authenticated from a foreign location while the admin himself on vacation.
WHO/ROLE: IT-Admin
ACCESS MODE: MFA-authenticated privileged login
BROKEN IAM PRINCIPLES: Zero-Trust, PAM, Context-Aware Access, MFA
HOW IT HAPPENED: though a malware, social engineering, phishing, account hijacking
POTENTIAL CONSEQUENCES:
- critical corruption of IT infrastructure
- data destruction or ransomware intent
- asset and data theft
- data as commodity- as soon stolen data enters the darknet, it risks being auctioned or sold to facilitate variety of crimes such as identity theft, financial crime, fraud, further attacks, credential stuffing, espionage, sabotage, disinformation etc
LOG INFO: Successful logon (4624), Logon using special credentials (4648), Special privileges assigned (4672) used in conjunction with 4624 to detect high privilege logon, Kerberos service ticket (4769) can show login mapping and the IP → look for successful MFA login, abnormal IP
WHY A PROBLEM: This is crucial security breach signaling insufficient protection around privileged account authentication and contextual access policies.

5. Customer data found on Common folder with everyone's Modify privileges in place

WHAT HAPPENED: An excel file with PII (Personally Identifiable Information) was stored in the Common folder where everyone has Modify access to.
WHO/ROLE: Unknown/ employed at the company
ACCESS MODE: Write
BROKEN IAM PRINCIPLES: Least Privilege, Personal Data Protection, Data Classification, Identify and Protect High Value Data
HOW IT HAPPENED: It happened because of reckless admin folder organization and privilege assignment, lack of DLP controls and data handling policy enforcement

POTENTIAL CONSEQUENCES:
- data leakage
- noncompliance and fine against data protection laws
- reputational damage

LOG INFO: File accessed (4663), Object handle requested (4656) → shows file access by person
WHY A PROBLEM: IAM was not enforced to ensure data-to-role alignment

6. Manager adds himself to Finance group

WHAT HAPPENED: A Manager managed to assign himself to Finance group
WHO/ROLE: Manager
ACCESS MODE: Write + Privilege Escalation
BROKEN IAM PRINCIPLES: RBAC principles, Separation of Duties, Least Privilege,
HOW IT HAPPENED: It happened likely thanks to misconfigured DACL on the Finance group (although the original text points to Read only) or more likely due to inherited privileges from parent folder/group.
POTENTIAL CONSEQUENCES:
- unwarranted access
- industrial espionage
- access to non-public, financial secrets can lead to insider trading
- data/ stock manipulation
- financial fraud
- data theft

LOG INFO: Member was added to security group (4728), User added to a local group (4732), User account changed (4781) → group change log; monitor activity on the manager account
WHY A PROBLEM: This is a critical RBAC violation that undermines the entire access model. It very likely points to deeper issue within AIM architecture such as inheritance or group nesting.

PART 3. RISK ANALYSIS

The 6 incidents as shown in the examples reveal systemic weaknesses in the ADC IAM posture. Even though the steps towards securing the system have been taken, they are insufficient to protect the company against prominent threats from the inside and the outside actors, the extent of which poses critical risks to the company's operations.
The incidents show specific vulnerabilities in the architectural design of the company's security as displayed by following: sharing access to sensitive information without the separation of data-role relationship, lack of protection against brute-force attacks, insufficient MFA authentication for critical workforce and lack of regular audit practices as well as stable tools allowing to conduct them. On the other spectrum of vulnerabilities lies privilege design which allow wide-scale over-privileging and lack of control over lifecycle management as well as poor authentication practices.

1. Lack of privilege control

Evidence: Everyone has Modify rights on the Common folder; Interns have Modify rights on Finance files; Manager self-adding capabilities to Finance group
Risk: Unauthorized access and modification at the very least can make faulty operational data enter company's calculations, which can unintentionally expose them to financial or tax crime allegations. It can affect the trust between clients, if the modified documents are relevant to B2B relationship. In more extreme cases we can look at data tampering, data theft and industrial espionage if data is being acquired or sold. Stolen financial data can also be used to conduct financial crime, fraud, insider trading and stock manipulation
Standards mapping: The case above represents the failure in enforcing Separation of Duties as observed in ISO 27001 Annex A 5.3. The control is designed to reduce the risk of fraud and error by

a single person. In addition, the above scenario violates the GDPR Art. 5 “Principles Relating to Processing of Personal Data” and GDPR Art. 32 “Security of Processing” where lack of privilege control can violate personal data. The above provision strives to ensure protection of personal data through “*the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services*” and adherence to “*regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing*”
Impact: High

2. Incorrect lifecycle management
Evidence: Ex-HR employee logging into work account while no longer working for the company.
Risk: Orphaned accounts present an attack vector for former employees and attackers looking to leverage stale credentials. This poses a risk of data exfiltration and sabotage under the radar.
Standards mapping: CIS Control6 & 8; ISO 27001 A.9.2.1 “User Registration and Deregistration” list steps in pursuit of effective user account creation as well as the necessity of auditing and periodic control reviews, neither of which took place in case of deprovisioning an old HR account.
Impact: High

3. Weak authentication
Evidence: Multiple login attempts into Finance account; MFA only present for admin roles
Risk: Risky but not sole cause of brute-force attacks, credential stuffing and account hijacking.
Standards mapping: NIST 03.05.03 “Multi-Factor Authentication” points to necessity of MFA on privileged and non-privileged users. ISO 27001 Annex A 8.5 “Secure Authentication” mandates login mechanisms such as MFA to prevent unwarranted access including brute force attack.
Impact: Medium (I put “medium” here, not higher because brute-force attacks are to be expected regardless of the size or character of the company. As these attacks are spontaneous and very often bot-inflicted, the security in place exceeds the reach of IAM configurations alone)

4. Lack of logging/monitoring
Evidence: PII stored in Common folder not detected; ex-HR account not deprovisioned and activity log not present; privilege-account logging from foreign location not blocked; no audit present for modified business docs by unsolicited employee.
Risk: Lack of logging and tracking facilities doesn’t prevent attackers from getting into the system but it allows them to stay there undetected, move laterally and cause persistent financial, legal and reputational damage.
Standards mapping: CIS Control 8; ISO 27001 9.2 “Internal Audit”- this clause requires companies to commit to regular audit and monitoring to assess their threat protection and prevention effectiveness.
Impact: Very high

5. Threats (insider threat, career sabotage, data leakage etc)
Evidence: Current security configuration enables multiple attacker profiles: negligent insiders (accident modification, data leak), malicious insiders (spying, theft, privilege abuse, data tampering), external attacker (brute-force attack, account hijacking) and organized financial crime (fraud, data theft, stock manipulation, insider trading) to operate in the environment.
Risk: Unless governance, lifecycle automation, universal MFA, PAM/JiT, and SIEM/response controls are implemented, residual risk remains critical.
Standards mapping: ISO 27001 Annex A 5.7 “Threat Intelligence”- this provision emphasizes on the need to gather intelligence on all possible threats and provide actionable solutions. To comply with the above standards the organizations must commit to regularly examining their work environment, determining the sources of threats, build an understanding of attack vectors and built systems to prevent them.
Impact: Critical

PART 4. IMPROVEMENT PROPOSAL

The incident patterns and risk landscape outlines so far demonstrate that ADC requires a strategic, standards-aligned overhaul of its IAM governance and technical controls. The following improvement proposals incorporate best practices from ISO 27001, NIST SP 800-53, CIS Controls, and regulatory requirements under GDPR.

1. IAM policy improvements

a) A role-driven, least privilege access and separation of duty
Recommendation: Conduct a full role and RBAC re-engineering, to ensure ALL departments have only minimum permissions necessary. Document all roles, ownerships and privileges.
STANDARDS: ISO 27001 A.9.1, NIST AC2, AC5, AC6, CIS Control 5 & 6, GDPR Art. 5

b) Privileged Access Management (PAM) and Just-in-Time (JiT) framework.
Recommendation: All admin roles should adopt JiT access framework, work-time limitations, geo-blocking and session recording. Permanent admin permissions should be deactivated.
STANDARDS: ISO 27001:2022 Annex A 8.2, NIST AC17, GDPR Art.32

c) High risk roles redesign
Recommendation: Exclude managers from self-appointed access. Require dual check for memberships in high risk/responsibility groups (Admin, Finance, HR)
STANDARDS: ISO 27001 Annex A.9, CIS Control 6

2. Privilege Management improvements (RBAC, JiT, PAM)

a) Monthly Access Reviews
Recommendation: Perform access and privilege reviews every 30 days for ALL groups highlighting excessive privileges.
STANDARDS: ISO 27001:2022 Annex A 5.22, NIST SI10 (2)

b) Strict enforcement of DACL/SACL and data classification
Recommendation: Reclassify ALL documents in the Finance, Admin and HR groups according to three tier classification (Internal, Confidential, Highly Restricted). Assign group-specific folder to facilitate sharing of file between users. Decommission the Common folder. Re-administer DACLs to align with data classification and SoD
STANDARDS: ISO 27001:2022 Annex A 8.12, ISO 27001:2022 Annex A 8.16, ISO 27001:2022 Annex A 5.12, CIS Control 3, GDPR Art.32 & Art.25

c) Emergency PAM and monitoring
Recommendation: Deploy break-glass accounts for admins with session logging
STANDARDS: ISO 27001:2022 Annex A 8.2, NIST AC2, CIS Control 17

3. Lifecycle Management automation

a) Automated on/offboarding
Recommendation: incorporate HRIS (Human Resources Information System) into AD. It uses employee data to automatically assign privileges and resources during the whole lifecycle. No manual steps for account provisioning/deprovisioning
STANDARDS: ISO 27001 Annex A.9, ISO 27001:2022 Annex A 6.5, NIST SI4, NIST SI18, GDPR Art.5(1)& Art.32

b) Identity Governance and Admin
Recommendation: Implement a governance engine such as Azure Entra ID Governance or alternative for automated control over user identities to ensure the right people have the right access.
STANDARDS: ISO 27001:2022 Annex A 8.27, NIST SR4

4. Authentication improvements

a) Universal MFA enforcement
Recommendation: Mandatory MFA for everyone, no exceptions. Phishing resistant MFA (FIDO2, WebAuthn, smartcards) for HR, Finance and Admin
STANDARDS: NIST IA2 (it's about MFA for privileged accounts, my recommendation is that everyone uses it), ISO 27001 Annex A 8.5, GDPR Art.32

b) Zero Trust over Conditional Access
Recommendation: Implement Zero-Trust policy over conditional access- block login from foreign countries, prevent installing non-compliant software, download from private USB and access/MFA from unknown devices
STANDARDS: NIST AC20, ISO 27001:2022 Annex A 8.12, ISO 27001:2022 Annex A 8.16, CIS Control 4

c) Brute-force attack defenses
Recommendation: Lock accounts after 10 failed attempts. Use RdpGuard or alternative to block IPs after failed login attempts. Consider throttling
STANDARDS: ISO 27001:2022 Annex A 8.16, ISO 27001:2022 Annex A 8.20, CIS Control 13

5. Logging and monitoring

a) Audit and monitor everything!
Recommendation: Implement audits for each performed action. Implement FIM (File Integrity Monitoring) on critical files for events like permissions changes, access, modifications, copies etc
STANDARDS: NIST SI4, ISO 27001:2022 Annex A 8.16, CIS Control 8

b) Data Loss Prevention (DLP)
Recommendation: Deploy a DLP solution on both endpoints and cloud environments to continuously monitor data to prevent exfiltration, mishandling and unwarranted access.
STANDARDS: ISO 27001:2022 Annex A 8.12, CIS Control 11, GDPR Art.32

c) SIEM integration
Recommendation: Forward all logs with alerts for suspect activity i.e. multiple failed logins, foreign IP, brute-force detection, privilege escalation, sensitive file modification etc to SIEM (Security Information and Event Management)
STANDARDS: ISO 27001:2022 Annex A 8.27, NIST SI4 (2), GDPR Art.33–34

6. Continuous threat awareness

a) Security training
Recommendation: Hold annual training for ALL employees regarding threats and malware awareness, importance of protecting one's credentials, handling sensitive and personal data
STANDARDS: ISO 27001:2022 Annex A 6.3, ISO 27001:2022 Requirements & Clauses – 7.3 Awareness, CIS Control 14

b) Intelligence gathering
Recommendation: Conduct regular threat reconnaissance regarding inside and outside danger factors, historic and hypothetical threats. Build a factual and data-driven database of cybersecurity risks and implement relevant defenses in a timely fashion
STANDARDS: NIST SI4,ISO 27001:2022 Annex A 5.7, CIS Control 7

c) Annual ISO/NIST-compliant audit
Recommendation: Conduct an annual check of all the security measures and critically asses their relevance as well as effectiveness against the ISO 27001 and NIST standards-aligned. Or better yet, get ISO-certified.
STANDARDS: ISO 27001:2022 Requirements & Clauses – 9.2 Internal Audit, CIS Control 18, GDPR Art.5, 25, 32

These improvements form a unified IAM strategy aligning AcmeDataCorp with recognized standards and legal requirements. By strengthening access governance, authentication, monitoring, and lifecycle management, the organization can significantly reduce risks of insider abuse, credential compromise, data leakage, and regulatory violations establishing a secure IAM environment.

SOURCES:

- https://www.isms.online/
- https://csrc.nist.gov/CSRC/media/Projects/risk-management/800-53%20Downloads/800-53r5/SP_800-53_v5_1-derived-OSCAL.pdf
- https://www.cisecurity.org
- https://www.cisecurity.org/controls/cis-controls-list
- https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx
- https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- https://csf.tools/