Improper Credential Sharing in Critical Information Systems Environments: A Technical-Operational Case Study on Loss of Traceability, Insider Risk, and Identity Control Measures

Margarida de Jesus *, Mario Monteiro Marques, Antonio Goncalves

Posted Date: 8 June 2026

doi: 10.20944/preprints202606.0570.v1

Keywords: credential sharing; identity management; insider risk; traceability; access control; multi-factor authentication; classified information; audit logging; operational security; critical information systems; identity governance; critical infrastructure protection

 doi:10.20944/preprints202606.0570.v1

Article

Improper Credential Sharing in Critical Information Systems Environments: A Technical-Operational Case Study on Loss of Traceability, Insider Risk, and Identity Control Measures

Margarida de Jesus [1,*], Mario Monteiro Marques [2] and Antonio Goncalves [2]

[1] Instituto Superior Técnico, University of Lisbon

[2] CINAV, Portuguese Naval Academy

* Correspondence: margarida.v.jesus@tecnico.ulisboa.pt

Abstract

This case study analyzes a security incident resulting from improper credential sharing within the Communications Operations Center (COC), a fictional environment responsible for processing classified information. The incident originated in an informal practice of sharing credentials between shift operators, driven by operational pressure, inadequate shift-transition procedures, and an organizational culture tolerant of procedural deviation. As a result, access traceability was compromised, audit records became non-attributable to individual users, and insider-risk exposure increased significantly. The situation was further aggravated by the absence of multi-factor authentication (MFA), the lack of concurrent session control, and insufficient monitoring and access-review procedures. The incident was detected after a SIEM alert identified simultaneous authenticated sessions associated with the same account on physically distinct workstations. Subsequent investigation revealed the systematic use of shared credentials over a fourteen-month period, which prevented the reliable attribution of individual actions. The study reconstructs the incident timeline, analyzes technical, procedural, physical, and human failures, performs a structured risk assessment, and proposes corrective and preventive measures aligned with recognized information security standards and best practices. The findings are particularly relevant for critical information systems environments, where failures in identity management and access control may directly affect operational continuity, accountability, resilience, and trust.

Keywords: credential sharing; identity management; insider risk; traceability; access control; multi-factor authentication; classified information; audit logging; operational security; critical information systems; identity governance; critical infrastructure protection

1. Introduction

Information security in environments processing classified information depends not only on the robustness of technical safeguards, but also on the effectiveness of the organizational, procedural, and human controls governing system use. In such environments, the protection of confidentiality, integrity, and availability — commonly referred to as the CIA triad — constitutes a fundamental requirement for mission continuity, preservation of institutional trust, and maintenance of operational security. Consequently, seemingly minor procedural deviations may progressively evolve into systemic failures with significant operational and security impact.

In critical information systems environments, identity management and access control mechanisms constitute foundational security controls. Failures affecting accountability, traceability, and authentication may compromise operational resilience, regulatory compliance, incident investigation capability, and trust in the overall security architecture.

 doi:10.20944/preprints202606.0570.v1

Within the domains of Information Security (INFOSEC) and Communications Security (COMSEC), a fundamental principle applies: all actions performed within systems processing classified information must be unequivocally attributable to a properly identified, authenticated, and authorized individual. This principle constitutes the foundation of individual accountability, auditability, non-repudiation, and incident investigation capability, while simultaneously supporting the need-to-know principle and the preservation of reliable digital evidence [1,2]. Improper credential sharing directly compromises these mechanisms because information systems register only logical identities without guaranteeing reliable correspondence with the physical identity of the individual performing a given action.

This case study analyzes a simulated scenario occurring within the Communications Operations Center (COC), a fictional operational environment in which improper credential sharing progressively evolved from an isolated practice into an informally normalized operational behavior among multiple operators. The case demonstrates how technical, procedural, organizational, and supervisory failures may interact over time, enabling the gradual degradation of access control, traceability, and operational oversight mechanisms. The situation became particularly critical when shared credentials enabled unauthorized access to classified information above the authorization level assigned to the involved operators.

The incident was formally detected after the Security Information and Event Management (SIEM) platform identified simultaneous authenticated sessions associated with the same account on physically distinct workstations. The subsequent investigation revealed the prolonged existence of credential sharing practices involving multiple operators, compromising approximately fourteen months of audit records and preventing the reliable attribution of individual actions.

The study demonstrates how the combination of procedural, technical, physical, human, and organizational failures may simultaneously compromise traceability, individual accountability, and the effectiveness of auditing mechanisms in environments processing classified information. Additionally, the study evaluates the adequacy of existing authentication, identity management, monitoring, and operational supervision controls, proposing corrective and preventive measures aligned with internationally recognized standards and information security best practices [1,2,4,5].

The presented scenario is entirely fictional and developed exclusively for academic purposes. It contains no real classified information and no references to actual individuals or organizations. Despite its simulated nature, the case was constructed based on recurring organizational failure patterns documented in the literature and on security frameworks applicable to INFOSEC/COMSEC operational environments [11,12].

2. Operational Context and Assumptions

2.1. Organizational Context

The COC is a fictional operations center responsible for the processing, routing, and archiving of classified communications exchanged between field units and national-level decision-making structures. The center operates continuously (24/7) through three rotating eight-hour shifts staffed by permanent operational teams.

The operational environment processes information with different classification levels: Level I (Restricted), Level II (Confidential), Level III (Secret), and Level IV (Top Secret), in increasing order of sensitivity and criticality. Information is stored and processed within a dedicated infrastructure composed of workstations connected to a protected network and servers segregated from external non-classified networks.

Under normal operational conditions, operators primarily access Level I and Level II classified information. Access to Level III information is restricted to personnel holding specific authorization and validated need-to-know, while access to Level IV information is limited to senior personnel possessing the appropriate security clearance and explicitly authorized privileges.

 doi:10.20944/preprints202606.0570.v1

Segregation between classification levels seeks to limit unnecessary exposure of sensitive information, thereby reducing the potential impact of unauthorized access and ensuring compliance with the need-to-know principle. This model also contributes to preserving the confidentiality, integrity, and availability of processed information [1,7].

The center operates under the authority of a Security Officer (SO), supported by a System Administrator (SA), a COMSEC Officer, and a hierarchical operational structure responsible for daily operational supervision. Access to classified systems is regulated through formal access control and classified information protection policies derived from national regulations applicable to the INFOSEC/COMSEC domain [7,8].

2.2. Assets and Dependencies

The execution of COC operational activities depends on a set of critical information, authentication, and monitoring assets whose availability, integrity, and traceability are essential to operational continuity.

The primary assets relevant to this case study include the classified communications repository, operator workstations connected to the protected network, the authentication and identity management infrastructure, session logging and monitoring mechanisms, removable media authorized for specific operational workflows, and the cryptographic key management system used to protect stored and transmitted information.

The classified information repository predominantly contains Level I and Level II information accessible to operators, as well as Level III information subject to additional access restrictions. The authentication and identity management infrastructure supports user identity validation, centralized credential management, and activity logging for auditing, compliance, and incident investigation purposes [6].

These assets depend directly on the Identity Management (IdM) platform, the Human Resources (HR) system, and the Security Information and Event Management (SIEM) infrastructure, which is responsible for the collection, correlation, and analysis of security events, as well as the automatic generation of operational security alerts.

The unavailability or compromise of these dependencies may directly affect the environment's authentication, traceability, monitoring, and operational supervision capabilities.

2.3. Actors and Responsibilities

Table 1 presents the principal actors involved in the analyzed scenario, together with their respective functions and relevant permissions.

Table 1. Actors, Functions, and Relevant Permissions.

Actor	Function	Relevant Permissions
Security Officer (SO)	Security governance, incident management, and policy authority	Access up to Level IV; access to audit records; approval of security policies and access management
System Administrator (SA)	System configuration, account management, and SIEM monitoring	Administrative privileges over systems and logs; no authorized access to Level III/IV operational content
COMSEC Officer	Management and supervision of the cryptographic key lifecycle	Access to cryptographic systems; authorized read access up to Level III
Operators (A, B, C, D)	Processing and routing of classified communications	Read/write access to Level I and II information; Level III access only under specific authorization
Internal Auditor (IA)	Compliance verification, access reviews, and log analysis	Read-only access to systems and logs for auditing and investigation purposes

 doi:10.20944/preprints202606.0570.v1

2.4. Access Rules and Classification Framework

Access to classified systems is governed by the need-to-know principle, with permissions assigned according to the user's operational role and security clearance level [1,2]. Any privilege of escalation requires formal approval from the appropriate chain of command and must be justified by operational requirements.

Functional compartmentalization restricts operators' access exclusively to the classification levels required for the execution of their duties, thereby reducing unnecessary information exposure and mitigating the potential impact of unauthorized access. Additionally, segregation of duties seeks to prevent the concentration of critical responsibilities within a single user or operational unit, reinforcing independent supervision mechanisms and reducing the risk of privilege misuse [3].

All access to systems is performed through credentials individually and non-transferably assigned to each user and centrally managed through the IdM platform, subject to complexity requirements, periodic renewal, and administrative control [4,5]. Credentials may not be shared, reused by third parties, or used outside the authorized operational context.

The systems also maintain logging and monitoring mechanisms intended to ensure reliable traceability of executed actions, including identification of the authenticated user, workstation utilized, timestamps, and accessed resources [6]. These records constitute an essential element for auditing, incident investigation, accountability, and compliance verification in environments processing classified information.

Additionally, security event monitoring is supported by the SIEM infrastructure, responsible for event correlation, anomaly detection, and generation of operational alerts whenever behaviors potentially incompatible with authorized account usage profiles are identified.

3. Case Description: Timeline and Evidence

This section describes the temporal evolution of the incident, the principal events identified during the investigation, and the evidence used to reconstruct activities associated with the improper sharing of credentials. The chronological analysis enabled the correlation of authentication events, physical access records, and operational activities, supporting the identification of control failures and the assessment of the operational impact resulting from the loss of traceability and accountability.

3.1. Incident Background

The practice of improper credential sharing within the COC began approximately fourteen months before its formal detection. During a period characterized by elevated operational tempo, temporary staffing shortages, and sustained pressure associated with mission continuity, several operators began informally sharing authentication credentials as a temporary mechanism to maintain continuity between consecutive operational shifts.

Initially limited to isolated shift-transition situations, the practice progressively evolved into a recurrent and informally normalized behavior within the operations center. The absence of effective technical enforcement mechanisms, combined with limited operational supervision and an organizational culture permissive toward procedural deviations, allowed the behavior to persist and gradually expand to multiple operators over time.

The subsequent investigation demonstrated that at least four operators regularly used credentials belonging to other personnel, including accounts associated with authorization levels exceeding their assigned permissions. One identified case involved an operator without Level III authorization using the credentials of a colleague with higher privileges, thereby enabling unauthorized access to classified documentation above the user's assigned authorization level. This situation constituted a direct violation of the need-to-know principle and significantly increased risks associated with insider threats, privilege misuse, loss of traceability, and compromise of individual accountability.

 doi:10.20944/preprints202606.0570.v1

The practice remained undetected for an extended period due to the absence of multi-factor authentication (MFA), the lack of simultaneous session control mechanisms, and insufficient periodic access review and monitoring procedures [4–6]. Additionally, the absence of effective correlation mechanisms between physical identity and logical identity significantly reduced the organization's ability to detect anomalous authentication behavior.

Initial detection occurred when the SIEM platform identified simultaneous authenticated sessions associated with the same account on two physically distinct workstations. The event represented an authentication pattern logically incompatible with the physical presence of a single operator and generated an automated alert subsequently escalated for investigation by the System Administrator (SA) and the Internal Auditor (IA).

3.2. Incident Timeline

The first identified instance of credential sharing occurred approximately fourteen months before the formal detection of the incident, during a period characterized by elevated operational workload and temporary staffing shortages. In order to maintain continuity of ongoing activities associated with the processing of Level II classified information, Operator A informally shared authentication credentials with Operator B during an extended shift transition. Although initially perceived as a temporary operational workaround, this practice marked the beginning of the gradual degradation of individual traceability within the operational environment.

Approximately two months later, the practice progressively expanded to additional personnel. Operators C and D began regularly using credentials belonging to Operators A and B, including accounts associated with authorization levels exceeding their own operational permissions. During this period, the first confirmed unauthorized access to Level III classified documentation occurred through the use of third-party credentials. Despite the seriousness of the violation, no formal report or escalation process was initiated.

Approximately ten months after the initial occurrence, the Identity Management (IdM) platform triggered the mandatory periodic password renewal process. Although credentials were formally changed, operators informally coordinated the sharing of the newly generated passwords, allowing the practice to continue without interruption or formal detection. This phase consolidated credential sharing as an operationally normalized behavior within the environment.

Formal detection of the incident occurred at 22:14 (T1), when the SIEM platform generated an alert after identifying simultaneous authenticated sessions associated with account OP_A on Workstation 03 and Workstation 07. The detected authentication pattern was logically incompatible with the physical presence of a single operator and was subsequently escalated for investigation by the SA and IA.

At 22:31 (T2), the SA physically confirmed the presence of Operator A at Workstation 03. The authenticated session identified on Workstation 07 was being actively used by Operator C, who admitted using Operator A's credentials to access Level II and Level III classified information. This event constituted the first direct confirmation of systematic credential sharing and improper privilege escalation within the operational environment.

At 23:05 (T3), the Security Officer (SO) was formally notified of the incident. The unauthorized session on Workstation 07 was immediately terminated, and accounts OP_A and OP_B were preventively suspended. Simultaneously, the formal incident management and containment process was initiated.

Three days later (T4), the Internal Auditor initiated a retrospective analysis of the available authentication and operational logs. The investigation concluded that approximately fourteen months of activities associated with accounts OP_A and OP_B could not be reliably attributed to specific individuals, significantly compromising auditability, accountability, and the integrity of the available audit records.

Ten days after the initial detection (T5), the final audit report formally confirmed the existence of systematic credential sharing practices, the absence of multi-factor authentication mechanisms,

 doi:10.20944/preprints202606.0570.v1

and the lack of effective controls preventing concurrent authenticated sessions. The incident was subsequently escalated to senior management as a systemic operational security failure requiring immediate corrective and preventive action.

3.3. Available Evidence

During the investigation, multiple sources of technical and documentary evidence relevant to the chronological reconstruction of the incident were identified, preserved, and analyzed. All relevant records were preserved in accordance with formal digital chain-of-custody procedures, including SHA-256 hash-based integrity verification, controlled access to collected artifacts, and documented preservation and analysis activities [6].

The primary evidence sources included SIEM records related to the simultaneous sessions identified during event T1, including workstation identifiers, timestamps, source addresses, and authentication metadata confirming concurrent use of the same logical identity across distinct terminals.

Authentication records obtained from the IdM platform covered approximately fourteen months of activity and included authentication events, session initiation records, and session termination logs associated with logical identifiers OP_A and OP_B. The investigation concluded that the majority of these records did not permit reliable association between logical identity and physical user, thereby compromising the principles of accountability, auditability, and non-repudiation [6].

Physical access control logs based on individual access cards enabled correlation between operator physical presence and logical access activity. These records revealed inconsistencies between physical location and account usage patterns, supporting the identification of unauthorized credential utilization.

Additional evidence included the formal statement provided by Operator C during the audit process, confirming the use of Operator A's credentials during event T2 to access Level II and Level III classified documentation. This statement constituted direct evidence of credential sharing and improper privilege escalation.

The investigation also analyzed access logs from the classified information repository, demonstrating recurrent use of accounts OP_A and OP_B to access Level I, Level II, and occasionally Level III documentation without reliable individual attribution. Furthermore, password renewal event logs from the IdM platform revealed coordinated password changes and temporal patterns consistent with the continued maintenance of shared credentials.

The investigation additionally identified several significant evidence gaps that limited the completeness of forensic reconstruction and early detection capabilities. These included the absence of MFA authentication records, the lack of automatic simultaneous session blocking mechanisms, the absence of behavioral monitoring mechanisms capable of identifying anomalous account usage patterns, ineffective periodic access and privilege review procedures, and the absence of previous alerts associated with concurrent credential usage.

No prior formal reports associated with improper account usage or suspected credential sharing practices were identified during the investigation, further demonstrating the prolonged normalization of the behavior within the operational environment.

4. Normative and Procedural Framework

4.1. Applicable Standards and Policies

The following regulatory and normative sources define the requirements applicable to identity management, access control, authentication, and accountability in environments processing classified information:

- **ISO/IEC 27001:2022 – Information Security Management Systems [1]:** Controls 5.15 (*Access Control*), 5.16 (*Identity Management*), 5.17 (*Authentication Information*), and 8.2 (*Privileged Access Rights*) establish requirements related to the individual assignment of access rights, protection

 doi:10.20944/preprints202606.0570.v1

of authentication information, appropriate privilege management, and unequivocal accountability for actions performed within information systems.

- **ISO/IEC 27002:2022 – Information Security Controls [2]:** Section 5.17 establishes that authentication information must not be disclosed or shared between users and requires the implementation of mechanisms ensuring secure individual authentication. Section 8.5 further reinforces requirements related to the secure use of information systems and the protection of authentication mechanisms.
- **ISO/IEC 27005:2018 – Information Security Risk Management [3]:** Defines principles and methodologies for information security risk assessment and treatment, including the identification of assets, threats, vulnerabilities, impacts, and mitigation measures. This framework supports the risk assessment presented in Section 5.3.
- **NIST Special Publication 800-53 Rev. 5 – Security and Privacy Controls for Information Systems and Organizations [4]:** Control IA-2 requires unique identification and authentication of individual users; control IA-5 establishes requirements for secure authenticator management, including the prohibition of credential sharing; and control AC-2 requires the use of individual accounts, formal account lifecycle management, and preservation of accountability mechanisms.
- **NIST Special Publication 800-63B – Digital Identity Guidelines [5]:** Provides technical guidance regarding authentication, credential management, and session management, including requirements related to multi-factor authentication (MFA), authenticator protection, and mitigation of risks associated with credential misuse.
- **NIST Special Publication 800-92 – Guide to Computer Security Log Management [6]:**

Defines requirements applicable to the collection, storage, protection, and analysis of security logs in information systems, directly supporting the assessment of the auditing and traceability deficiencies identified in this case study.

- **Council Decision 2013/488/EU [7]:** Establishes security principles applicable to the protection of European Union classified information, requiring strict access control, individual accountability, and the maintenance of records enabling the reliable attribution of actions to be identified users.
- **GNS NT-E 04 – Access to Classified Information: Need-to-Know Principle [8]:** Defines national requirements applicable to access to classified information, including individual authorization, validation of need-to-know, and prohibition of informal use of third-party credentials.
- **COC Internal Access Control Policy (simulated):** Explicitly prohibits the use of shared or generic accounts, establishes periodic access reviews, and mandates the use of multi-factor authentication for access to classified information systems.

4.2. Applicable Security Requirements

Based on the normative and procedural framework identified above, the following minimum security requirements apply to the present case:

1. **Individual identification:** Each user must possess a unique individual account unequivocally associated with their physical identity. The use of shared or generic accounts is strictly prohibited [1,4].
2. **Strong authentication:** Access to systems processing classified information must be protected through multi-factor authentication (MFA), using at least two independent authentication factors (knowledge, possession, or inherence) [5].
3. **Logging and traceability:** Systems must maintain complete and reliable records of performed activities, including user identification, workstation used, timestamps, and accessed resources, enabling chronological reconstruction of executed actions [6].
4. **Session control:** Technical mechanisms must exist to prevent, limit, or automatically flag simultaneous use of the same account across different terminals, enabling immediate detection of anomalous usage patterns [4].

 doi:10.20944/preprints202606.0570.v1

5. **Credential protection:** Authentication policies must ensure that credentials are used exclusively by their assigned owner, prohibiting disclosure, reuse, or sharing between users [2,5].
6. **Access management:** User privileges must be limited to the minimum necessary for the performance of assigned duties and must be subject to periodic review and formal validation by the appropriate chain of command, in accordance with the principle of least privilege [1].
7. **Incident reporting:** Any suspected misuse of credentials, violation of authentication policies, or anomalous behavior must be immediately reported to the responsible security authorities, enabling timely response and containment actions [7,8].

5. Technical and Operational Analysis

The technical and operational analysis of the incident identified a set of interdependent procedural, technical, physical, human, and organizational failures that collectively compromised the traceability, individual accountability, and access control mechanisms of the operational environment. The incident further demonstrates the simultaneous failure of multiple defense layers, highlighting that the mere existence of security policies is insufficient in the absence of effective implementation, monitoring, enforcement, and continuous compliance verification mechanisms.

The investigation demonstrated that the credential sharing practice did not result from a single isolated technical vulnerability, but rather from the progressive combination of organizational deficiencies, absence of compensating controls, and operational normalization of insecure behaviors over time.

5.1. Identification of Failures

5.1.1. Procedural Failures

The most significant procedural failure corresponded to the absence of effective mechanisms designed to enforce compliance with policies prohibiting credential sharing. Although internal access control policies explicitly prohibited the use of shared accounts, no formal procedures existed for systematic compliance verification, behavioral supervision, or structured reporting of policy violations [1,2].

The absence of a formal shift-transition procedure requiring session termination and individual reauthentication directly contributed to the continued misuse of credentials between operators. During periods of elevated operational workload, operators frequently relied on maintaining authenticated sessions or informally sharing passwords to ensure immediate continuity of ongoing tasks.

The periodic password renewal process managed through the IdM platform also revealed significant limitations. Although periodic credential changes were mandatory, the process did not include mechanisms capable of validating that newly created passwords remained under the exclusive control of their assigned owners. Consequently, password renewal did not interrupt the credential-sharing practice, allowing it to persist across successive authentication cycles [5].

Additional deficiencies were identified regarding operational supervision and compliance auditing focused on verifying the individual use of accounts. Existing periodic access reviews were limited to formal validation of assigned privileges and did not include mechanisms capable of detecting concurrent, anomalous, or unauthorized use of digital identities [3].

5.1.2. Technical Failures

Multiple technical failures were identified that enabled and perpetuated credential misuse within the analyzed operational environment.

Absence of Multi-Factor Authentication (MFA): The authentication model relied exclusively on username and password credentials, making possession of the password sufficient to fully assume another operator's digital identity. The absence of MFA eliminated an additional layer of identity

 doi:10.20944/preprints202606.0570.v1

verification, enabling unauthorized access to classified information, including Level III documentation [5].

Absence of Concurrent Session Control: The IdM platform did not implement mechanisms capable of limiting, blocking, or automatically flagging simultaneous authenticated sessions associated with the same account. As demonstrated during event T1, account OP_A remained active simultaneously on two distinct workstations without automatic session termination or immediate blocking [4].

Inadequate SIEM Configuration: The investigation revealed that detection rules previously configured to identify concurrent authentications had been temporarily disabled due to the excessive number of false positives generated during periods of elevated operational activity. This inadequate configuration created a prolonged period during which anomalous authentication patterns remained undetected [6].

Absence of Behavioral Monitoring: The operational environment lacked behavioral analysis and advanced event-correlation mechanisms capable of identifying patterns inconsistent with legitimate account usage. Undetected behaviors included simultaneous use of the same account from different locations, access outside the expected operational profile, recurrent access to documentation incompatible with the user's authorization level, and anomalous authentication patterns during operational transition periods.

Insufficient Correlation Between Physical and Logical Identity: Existing systems did not ensure automatic correlation between physical access records and logical authentication events at operational workstations. This limitation significantly reduced the capability for early detection of inconsistencies between physical presence and authenticated activity [6].

5.1.3. Physical Failures

Existing physical security controls were limited to individual badge-based access to the operations room, with no complementary identity validation mechanisms implemented at workstation level. Consequently, any operator with legitimate physical access to the facility could use credentials belonging to another user without encountering additional authentication barriers.

The physical layout of the operational environment and the continuous use of workstations across shifts also facilitated the persistence of authenticated sessions after operator changes. In multiple situations, authenticated sessions remained active during operational transitions, enabling immediate continuation of activity under the previously authenticated account.

Operational supervision during periods of reduced activity, particularly during night shifts, proved insufficient to ensure timely detection of improper behavior. The reduced presence of direct hierarchical supervision significantly decreased the probability of informal identification of credential-sharing practices.

5.1.4. Human and Organizational Failures

Human failures manifested at both individual and organizational levels. The operators involved consciously chose to share credentials, justifying the practice based on operational continuity requirements and time pressure within the operational environment.

The prolonged repetition of the behavior contributed to its informal normalization among operators, progressively reducing the perception of risk associated with improper account usage. The absence of disciplinary consequences, combined with the lack of formal detection for approximately fourteen months, reinforced the perception that the practice was operationally acceptable [13].

The investigation also demonstrated insufficient awareness and training regarding traceability, individual accountability, non-repudiation, and protection of digital identities. Although operators formally acknowledged the existence of access control policies, they significantly underestimated the operational, legal, and security consequences associated with the loss of correspondence between physical and logical identity.

 doi:10.20944/preprints202606.0570.v1

At the organizational level, informal tolerance toward procedurally non-compliant but operationally convenient behaviors created an environment conducive to the gradual degradation of control mechanisms and security culture.

5.2. Causal Analysis

The root cause of the incident corresponded to the organizational failure to provide technical and procedural mechanisms capable of ensuring operational continuity without requiring credential sharing practices.

The investigation identified multiple contributing factors that favored the persistence and expansion of the practice over time, namely: a permissive organizational culture regarding procedural deviations; absence of multi-factor authentication [5]; lack of concurrent session control mechanisms [4]; insufficient behavioral monitoring capabilities; temporary deactivation of SIEM detection rules [6]; absence of audits focused on verifying individual account usage; and insufficient operational supervision during periods of reduced activity.

Existing control barriers proved either insufficient or inadequately implemented. The access control policy was formally established, but no effective mechanisms existed to verify compliance [1,2]. Although the SIEM platform possessed the technical capability to detect anomalous authentication patterns, inadequate rule configuration significantly reduced its operational effectiveness. Similarly, periodic access reviews were limited to administrative validation of assigned privileges and were not designed to identify shared use of digital identities [3].

5.3. Risk Assessment

The risk assessment was conducted considering likelihood and impact, in accordance with the principles established in ISO/IEC 27005:2018 [3]. Likelihood was estimated based on exposure duration, frequency of occurrence, number of operators involved, and absence of effective compensating controls. Impact was assessed considering the potential compromise of classified information confidentiality, integrity of control and auditing mechanisms, individual accountability, regulatory compliance, and incident investigation capability.

The identified scenarios demonstrate that credential misuse simultaneously affected the protection of classified information, the reliability of audit mechanisms, and the institutional capability to unequivocally attribute individual actions. Table 2 summarizes the primary risk scenarios identified.

Table 2. Risk Assessment.

Risk Scenario	Likelihood	Impact	Risk Level	Priority
Unauthorized access to Level II and Level III classified documentation by operators without appropriate authorization	High	High	CRITICAL	P1
Compromise of traceability, individual accountability, and auditing capability due to the inability to reliably attribute actions	High	High	CRITICAL	P1
Reputational exposure and non-compliance with regulatory requirements applicable to classified information handling	High	Medium	HIGH	P2
Unauthorized privilege escalation through credentials belonging to operators with higher authorization levels	Medium	High	HIGH	P2

 doi:10.20944/preprints202606.0570.v1

Abuse of authenticated sessions for malware introduction or information exfiltration by internal or external actors	Medium	High	HIGH	P2
Continued credential misuse without timely detection due to monitoring deficiencies and insufficient operational supervision	Medium	Medium	MEDIUM	P3

6. Corrective and Preventive Measures

6.1. Corrective Measures (Short-Term)

The corrective measures presented below are intended to support immediate incident containment, preservation of digital evidence, restoration of minimum operational security controls, and reduction of ongoing exposure associated with improper credential usage.

Table 3. Corrective Measures.

Measure	Responsible	Verification	Acceptance Criteria
C1: Immediate suspension of compromised accounts, forced credential reset, and temporary assignment of individual accounts to the involved operators	SA and SO	IdM account status records; incident ticket; formal authorization issued by the SO	Zero active sessions associated with suspended accounts and all operators authenticated exclusively through individually assigned credentials within 24 hours
C2: Full preservation of audit logs and relevant digital artifacts, including SHA-256 integrity validation and formal establishment of digital chain of custody procedures	IA and SA	SHA-256 hash records; signed chain-of-custody documentation; evidence of secure evidence storage	Integrity of collected records validated through cryptographic hashing and evidence protected against unauthorized modification
C3: Comprehensive review of existing accounts and removal of generic, shared, orphaned, or non-attributable accounts	SA and SO	Account review report; IdM deactivation records	All active accounts uniquely associated with individually identifiable users and absence of active generic or shared accounts
C4: Temporary enforcement of mandatory session termination and individual reauthentication during shift transitions	SA	Session termination records; operational validation logs	Absence of persistent authenticated sessions after operator transitions during the initial monitoring period

6.2. Preventive Measures (Medium- and Long-Term)

The preventive measures presented below are intended to eliminate the structural vulnerabilities identified during the investigation by strengthening authentication, traceability, operational monitoring, governance, and regulatory compliance mechanisms.

Table 4. Preventive Measures.

Measure	Responsible	Verification	Acceptance Criteria

 doi:10.20944/preprints202606.0570.v1

P1: Mandatory implementation of MFA for all access to Level II or higher systems, including physical token authentication for Level III and Level IV access [5]	SA and SO	MFA activation records within the IdM platform; SIEM authentication events	All Level II or higher accounts protected through MFA and absence of single-factor authentication events
P2: Implementation of concurrent session control mechanisms and automatic alert generation for simultaneous authentications [4]	SA	Configuration records; test reports; SIEM documentation	Automatic blocking of concurrent secondary authentication attempts and alert generation within ≤ 60 seconds
P3: Implementation of automated account lifecycle management integrated with HR and IdM systems [1]	HR and SA	Synchronization records; automatic deactivation reports	Absence of active accounts associated with inactive, transferred, or terminated personnel
P4: Enhancement of audit logging through mandatory recording of user identifier, workstation identifier, timestamp, accessed classification level, and session metadata [6]	SA and IA	Logging policy; sample log review; retention validation report	All logs contain mandatory audit fields and comply with defined retention requirements
P5: Implementation of behavioral monitoring and authentication anomaly detection mechanisms	SA	Behavioral baseline reports; generated alerts; technical documentation	Automatic detection and alerting of authentication patterns incompatible with the expected operational profile
P6: Mandatory training and awareness program covering credential management, traceability, insider threat risk, individual accountability, and reporting obligations	SO and Training Officer	Training attendance records; assessment results; approved training materials	All personnel trained with a minimum assessment score of 70%
P7: Formal establishment of proportional disciplinary procedures and implementation of a secure reporting channel, including anonymous reporting capabilities	SO, HR, and Legal Department	Published policy; communication evidence; reporting channel validation	Policy formally acknowledged by all personnel and operational validation of the reporting channel completed
P8: Quarterly independent audits of access management, authentication controls, logging, and regulatory compliance [3]	IA and SO	Audit reports; corrective action plans	Four complete audits conducted annually and absence of unresolved critical non-conformities

 doi:10.20944/preprints202606.0570.v1

P9: Progressive implementation of continuous identity validation mechanisms and reinforced enforcement of the principle of least privilege	SA and SO	Privilege review reports; segmentation reports; revised access control policies	Reduction of excessive privileges and continuous validation of privileged access activities

The proposed measures collectively address the procedural, technical, organizational, and monitoring deficiencies identified during the investigation. Their integrated implementation is intended to restore reliable traceability, reinforce individual accountability, reduce insider threat exposure, and strengthen the overall resilience of the operational environment against future credential misuse incidents.

7. Lessons Learned and Applicability

7.1. Lessons Learned

The primary lesson derived from this case is that technical controls and organizational culture must continuously reinforce one another. The existence of formal policies prohibiting credential sharing is insufficient in the absence of effective enforcement, monitoring, and accountability mechanisms. When operators perceive that procedural deviations do not result in consequences, such behaviors tend to become progressively normalized, particularly in environments characterized by sustained operational pressure [11,12].

The case also highlights the critical relationship between traceability and operational security. The inability to reliably associate actions with specific users directly compromises the organization's capacity to detect, investigate, and appropriately respond to security incidents. The loss of approximately fourteen months of reliably attributable records represents a substantial degradation of auditability, non-repudiation, and incident investigation capability [6].

Another important lesson concerns the management of monitoring mechanisms. The temporary deactivation of alerts or detection controls, even when motivated by legitimate operational requirements, should be governed by formal risk management procedures, including documented justification, explicit approval, implementation of compensating controls, and a formally defined reactivation deadline [3].

Finally, the case demonstrates that credential sharing frequently originates from structural limitations within operational processes. When authentication and shift-transition mechanisms fail to adequately support mission requirements, operators tend to develop informal workarounds to maintain operational continuity. In such contexts, eliminating structural causes is generally more effective than relying exclusively on disciplinary or awareness measures [11].

7.2. Recurring Failure Patterns

The failures identified in this case follow a recurring pattern commonly observed in organizational environments: a deviation initially justified by operational necessity gradually evolves into a tolerated practice, subsequently becomes normalized, and eventually becomes embedded within routine operational processes [13].

This pattern is particularly evident in high-tempo environments, where mission continuity is frequently prioritized over strict adherence to security procedures. Under such conditions, any degradation of individual accountability or traceability should be treated as a security event requiring mandatory reporting and immediate intervention, rather than an acceptable operational adaptation [7,8].

 doi:10.20944/preprints202606.0570.v1

The case further illustrates how the prolonged absence of detection mechanisms or supervisory intervention may reinforce the perception that insecure practices are operationally acceptable. Over time, this normalization process contributes to the progressive erosion of procedural discipline and weakens the effectiveness of existing security controls.

7.3. Transferability to Other Contexts

The conclusions of this case study are applicable to a wide range of environments handling classified or sensitive information, particularly contexts characterized by continuous operations, multiple shifts, and intensive use of centrally authenticated systems. The proposed measures such as including multi-factor authentication, concurrent session control, centralized identity management, behavioral monitoring, and periodic independent audits, are directly transferable to governmental, military, law enforcement, and critical infrastructure environments [9,10].

The case also reinforces the growing relevance of Zero Trust principles, particularly continuous identity verification, contextual access validation, and the assumption that authenticated access alone should not be considered inherently trustworthy in high-security operational environments.

It is important, however, to recognize the inherent limitations of this study. As a fictional and controlled scenario, the case assumes a relatively linear causal chain. In real-world environments, incidents of this nature typically involve multiple interdependent factors, organizational variability, legacy technical constraints, and more complex operational conditions. Consequently, this study should be interpreted as representative of a recurring organizational failure pattern rather than as an exhaustive representation of all possible sources of insider risk.

8. Conclusion

This case study demonstrated that improper credential sharing in environments processing classified information constitutes a systemic security failure with direct impact on traceability, individual accountability, auditability, and non-repudiation. The analyzed scenario illustrates how a deviation initially perceived as a temporary operational workaround may progressively evolve into a normalized informal practice, ultimately compromising fundamental principles of operational security and access control.

The investigation demonstrated that the loss of reliable correspondence between physical identity and logical identity directly compromises the ability to unequivocally attribute actions performed within classified systems. In the analyzed case, the continued use of shared credentials enabled unauthorized access to Level II and Level III classified documentation, prevented the reliable attribution of approximately fourteen months of operational activity, and significantly degraded the reliability and evidentiary value of available audit records.

The technical and operational analysis identified complementary procedural, technical, physical, human, and organizational failures, including the absence of multi-factor authentication, the lack of effective concurrent session control mechanisms, deficiencies in monitoring and supervision processes, and the informal normalization of procedural deviations. Collectively, these factors revealed a systemic failure of the defense-in-depth model, in which multiple layers of security controls proved insufficient to prevent, detect, or contain improper credential usage.

The risk assessment confirmed the existence of critical scenarios associated with unauthorized access to classified information, loss of traceability, and degradation of incident investigation capability, as well as high-risk scenarios related to privilege escalation, regulatory non-compliance, insider threat exposure, and malicious exploitation of authenticated sessions.

The proposed corrective and preventive measures were designed to directly address the identified vulnerabilities by simultaneously strengthening authentication, monitoring, auditing, governance, and operational supervision mechanisms. Their integrated implementation would restore individual accountability for system access, reinforce operational traceability, and significantly reduce the likelihood of recurrence of similar incidents.

 doi:10.20944/preprints202606.0570.v1

From a critical information systems perspective, effective identity governance, individual accountability, and reliable traceability mechanisms represent essential security requirements. The case demonstrates that seemingly routine procedural deviations, such as credential sharing, may generate systemic risks capable of affecting the security, resilience, and operational assurance of critical information systems.

Finally, the case demonstrates that the effective protection of INFOSEC/COMSEC environments depends on the continuous integration of technical controls, organizational processes, operational supervision, and security culture. In environments processing classified information, operational security cannot rely exclusively on declarative policies; it requires continuously enforced, measurable, and verifiable control mechanisms capable of maintaining trustworthy identity attribution throughout the operational lifecycle.

Abbreviations

IA	Internal Auditor
SA	System Administrator
CIA	Confidentiality, Integrity, and Availability
COC	Communications Operations Center
COMSEC	Communications Security
IdM	Identity Management
INFOSEC	Information Security
ISO	International Organization for Standardization
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
SO	Security Officer
HR	Human Resources
SHA-256	Secure Hash Algorithm 256-bit
SIEM	Security Information and Event Management
SP	Special Publication
EU	European Union

References

1. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.
2. International Organization for Standardization. (2022). *ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls*. ISO.
3. International Organization for Standardization. (2018). *ISO/IEC 27005:2018 — Information technology — Security techniques — Information security risk management*. ISO.
4. National Institute of Standards and Technology. (2020). *NIST Special Publication 800-53 Rev. 5: Security and privacy controls for information systems and organizations*. NIST.
5. National Institute of Standards and Technology. (2020). *NIST Special Publication 800-63B: Digital identity guidelines — Authentication and lifecycle management*. NIST.
6. National Institute of Standards and Technology. (2006). *NIST Special Publication 800-92: Guide to computer security log management*. NIST.
7. Council of the European Union. (2013). Decision 2013/488/EU on the security rules for protecting EU classified information. Official Journal of the European Union.
8. Gabinete Nacional de Segurança. (2024). *NT-E 04 — Acesso à informação classificada: Necessidade de conhecer*. GNS.

 doi:10.20944/preprints202606.0570.v1

9. European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024*. ENISA.
10. Cybersecurity and Infrastructure Security Agency. (2020). *Insider threat mitigation guide*. CISA.
11. Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124–133.
12. von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102.
13. Verizon. (2024). *2024 Data breach investigations report*. Verizon Business.