WHITE PAPER: BALANCING SECURITY AND USABILITY — INTEGRATING IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT AND SEGREGATION OF DUTIES IN A ZERO TRUST FRAMEWORK

by Mythili Arun

EXECUTIVE SUMMARY

In the evolving cybersecurity landscape, integrating Identity, Credential, and Access Management (ICAM) with Segregation of Duties (SoD) is a critical component of a Zero Trust Architecture (ZTA).

As government and enterprise environments accelerate adoption of ZTA, the intersection of ICAM and SoD is become increasingly critical. ICAM ensures users are accurately identified, authenticated, and appropriately authorized, while SoD is a risk management control that thwarts fraud by preventing any single individual from controlling multiple stages of a critical process.

Although both domains reinforce the Zero Trust principle of least privilege, organizations often struggle to implement SoD without degrading usability or creating operational friction. This white paper explores how ICAM and SoD can be integrated to achieve a balanced, secure, and efficient operating environment, supported by leading public sector and industry standards. The approach outlined herein not only supports compliance but also reduces audit findings, improves resilience to operate in an already complex threat-leaden architecture, and assists in making rapid access decisions.

This white paper offers practical integration approaches, governance and automation themes, and alignment with recognized industry standards.

INTRODUCTION: THE SHIFT TOWARD ZERO TRUST

As more government and enterprise systems adopt ZTA, the integration of ICAM and SoD becomes more important. ZTA emphasizes the principle of least privilege, which aligns directly with SoD. Least privilege limits user access to only those areas necessary to perform one's job. The shift toward ZTA is to alleviate audit pressures, respond to Department of Government Efficiency (DOGE) eliminations, and stem increases in insider risk threats.

ICAM is a comprehensive framework that manages who is accessing what, when, why, and how. ICAM thus provides security, accountability, and policy enforcement. SoD, on the other hand, ensures a critical process is not fully controlled by a single individual. It thereby reduces the risk of misuse, error, or fraud.

Federal agencies and enterprises are modernizing their cybersecurity strategies in alignment with mandates such as Executive Order 14028, Office of Management and Budget Memorandum M-22-09 (OMB M-22-09), and National Institute of Standards and Technology Special Publication (NIST SP) 800-207, which collectively define expectations for Zero Trust maturity. ZT shifts organizations away from implicit trust toward continuous verification, guided by real-time context and risk signals.

A foundational pillar of this transformation is identity. NIST identifies identity as the "new perimeter," making ICAM essential to enforcing Zero Trust access decisions (NIST SP 800-207; NIST SP 800-63-4). Simultaneously, SoD remains a longstanding internal control requirement across financial, human resource (HR), and mission systems. Frameworks such as OMB Circular A-123, Government Accountability Office Green Book (GAO-14-704G), and ISO/IEC 27001:2022 identify SoD as a core safeguard to mitigate fraud, insider threats, and operational misuse.

Despite their shared reliance on least privilege, ICAM and SoD are often implemented separately, leading to misaligned controls and gaps in governance. This white paper provides integration strategies between governance and tech controls, reducing operational friction.

UNDERSTANDING ICAM AND SoD

ICAM Components

Three components are operative within ICAM:

1. **Identity Management:** Creation, maintenance, and lifecycle management of digital identities.
2. **Credential Management:** Issuance, provisioning, and revocation of credentials.
3. **Access Management:** Authentication, authorization, and policy enforcement to ensure appropriate access decisions.

Governance is a critical factor in ensuring design and implementation of effective controls and consistency across ICAM implementations as well as oversight, reporting, compliance, and alignment with enterprise policies.

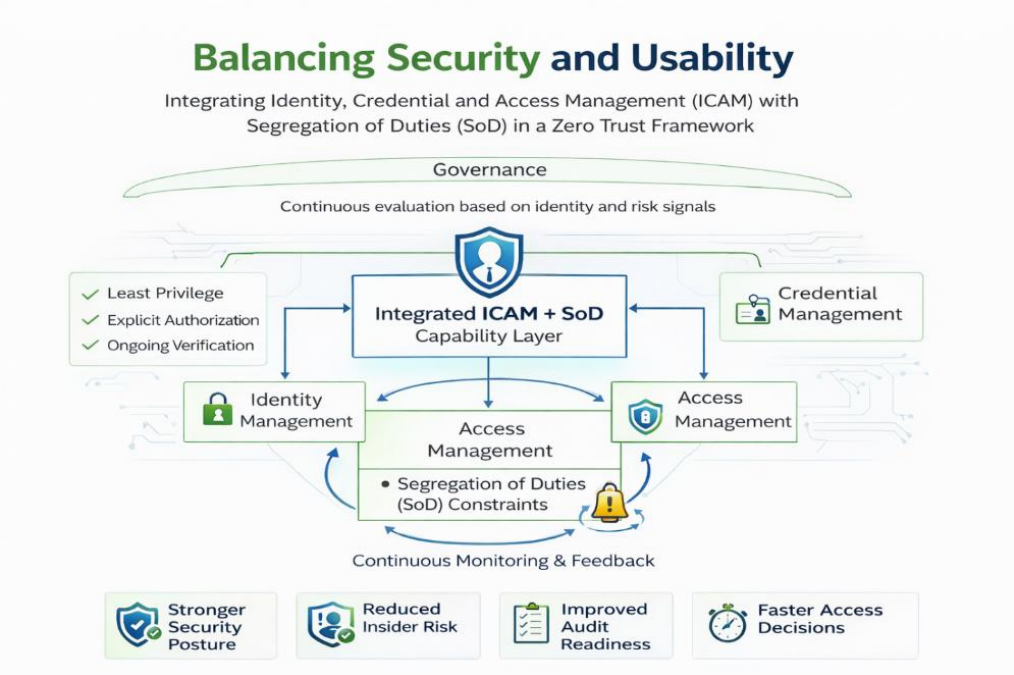
Together, these components enable the Zero Trust principles of continuous verification, least privilege, and explicit access authorization (NIST SP 800-207, §3).

Segregation of Duties

SoD is a risk management concept wherein misuse is prevented by dividing duties. It employs role-based access and clear task delineation. Most often, SoD is used to prevent fraud in HR, financial, mission, operational, and procurement systems. Standards such as OMB A-123, GAO-14-704G, and ISO/IEC 27001:2022 Annex A.6.1.2 emphasize that no single actor should be able to execute and approve critical transactions end-to-end.

Common examples include:

- A user who initiates a procurement action cannot approve or release funds.
- A system administrator cannot audit their own system activities.
- A payroll processor cannot create and approve employee wage adjustments.



Intersection of ICAM and SoD

As the figure illustrates, ICAM and SoD intersect in the following ways:

1. **Access Control:** SoD is enforced through integrated ICAM role definitions and permission sets. Role definitions within ICAM determine which duties cannot exist (NIST SP 800-162; SP 800-53, AC-5 & AC-6).
2. **Policy Enforcement:** ICAM systems can detect and prevent SoD violations automatically through Attribute-Based Access Control (ABAC) or Role-Based Access Control (RBAC) or a hybrid solution (NIST SP 800-162).

3. **Audit and Compliance:** Continuous monitoring, event logging, and access reporting support SoD requirements for audit readiness (NIST SP 800-53, AU-2 & AU-6; OMB A-123).

ICAM and SoD are mutually reinforcing: the stronger the identity architecture, the more reliable and enforceable SoD controls become.

KEY CHALLENGES

Implementing SoD within ICAM environments presents three key challenges:

1. *Balancing Security and Usability:* The more secure the system, the harder navigation can become for users. Complex rule enforcement may restrict users from performing legitimate job functions. Such restrictions will affect productivity and operational efficiency. NIST emphasizes usability as a critical factor in identity workflows (NIST SP 800-63-4, Appendix A). Overly restrictive access controls may force users into workarounds or create operational bottlenecks.
2. *Managing Complex Role Assignments:* Users may hold multiple roles across different applications or enterprise units. Without centralized oversight, it becomes difficult to identify conflicting access rights, especially when duties span systems, resulting in fragmented, inconsistent role structures. NIST SP 800-53 warns that insufficient oversight heightens the risk of privilege creep (AC-2 & AC-3).
3. *Organizational Barriers:* Resistance to change and siloed operations, lack of SoD awareness, and resistance to centralized governance are significant obstacles that impede effective implementation. Departments may be reluctant to relinquish control or collaborate on cross-functional governance. Many users are unaware of SoD conflicts unless they surface during audits or enterprise-level reviews. GAO identifies management buy-in as a prerequisite for internal control success (GAO-14-704G).

SOLUTIONS

Organizations should adopt a strategic approach that combines technology, governance, and cultural transformation to overcome these challenges.

1. Define Enterprise-Level SoD Rules

- Establish consistent SoD policies across all systems and departments through SoD conflict matrices across the organization.
- Create a centralized SoD ruleset repository to identify and manage conflicts holistically (aligned with NIST SP 800-53, PM-11).

- Account for cross-application role conflicts (e.g., initiating a transaction in one system and completing it in another).
- Establish enterprise policies that override local application expediency or promote policies in silos.

2. Involve Stakeholders to Change Mindsets

- Engage process owners, application owners, users, and auditors in defining SoD rules.
- Promote education and training around SoD to drive understanding of its business impact (OMB A-123, Appendix A).
- Empower stakeholders by making them part of the solution – not just subject to rules – and shift culture from compliance to risk-based governance.

3. Implement Adaptive ICAM Systems

- Move beyond static role-based access models to dynamic, context-aware access decisions based on device posture, location, risk, and identity confidence (NIST SP 800-207, §3).
- Continuously evaluate and simplify role definitions to reduce SoD conflicts by tailoring access to situational needs instead of static roles.

4. Automate SoD Checks

- Integrate SoD enforcement directly into ICAM workflows.
- Perform automated conflict detection at both the application and enterprise level.
- Use policy engines to dynamically prevent access that violates SoD policies.
- Implement policy engines to detect conflicts in real time (NIST SP 800-162).
- Support both pre-access (preventive) and in-session (detective/real-time) controls.

5. Embrace Continuous Monitoring

Continuous monitoring is central to Zero Trust (OMB M-22-09; NIST SP 800-207). Organizations should:

- Conduct periodic reviews and real-time access audits on a regular basis.
- Empower business and IT stakeholders to review SoD violations regularly through user-friendly dashboards and enterprise-wide reporting metrics.

- Ensure system-generated reports are actionable and easy to understand.
- Enable risk-based remediation workflows.

EMERGING TRENDS AND FUTURE CONSIDERATIONS

AI & Machine Learning in ICAM

- Leverage artificial intelligence (AI) to detect anomalous access patterns and predict potential SoD violations. Ensure AI augments human governance rather than replaces it. The AI model risk bias and explainability are foundational to ensuring auditability, regulatory compliance, and stakeholder trust. The combination of AI and human governance will be a success factor for SoD effectiveness, audit readiness, and access assurance.
- Use Machine Learning (ML) to refine roles over time based on actual user behavior and risk profiles (aligned with NIST AI RMF 1.0 guidelines).

Zero Trust and SoD Alignment

- SoD embodies the Zero Trust principle of trust no one implicitly, reinforcing controls against insider threats and fraud.
- ICAM-governed SoD will be a mandatory control capability as agencies advance toward the ZTA maturity levels outlined in OMB M-22-09.
- SoD enforcement must become continuous and identity centric as access decisions become more dynamic.
- Manual SoD reviews will not scale in mature ZTA environments.
- ICAM-governed SoD is an enabler of Zero Trust and not merely a compliance obligation. It must become entrenched within the organization.

Regulatory and Operational Compliance

- Future frameworks will demand deeper integration of SoD within enterprise ICAM solutions. As SoD becomes ingrained into organizations, they will move from a reactive remediation and band-aid fixes to a more mature, proactive integration and alignment of enterprise policies and governance.
- Organizations must prepare for evolving standards and increasing audit scrutiny.
- Reinforcing fragmented SoD implementation is untenable as oversight and monitoring increase.

CONCLUSION

As organizations transition to Zero Trust, integrating ICAM and SoD will not merely be a security best practice. It will be a necessity to maintain operational integrity, prevent fraud, and meet regulatory and audit requirements. Achieving this integration, however, will require more than technology alone. It will demand enterprise-wide collaboration, a deliberate shift in mindset, and sustained investment in automation, governance, and continuous monitoring.

By establishing clear policies, engaging stakeholders across the organization, and leveraging adaptive ICAM capabilities, organizations can strike the appropriate balance between security and usability, while strengthening operational effectiveness in the digital age. Ultimately, ICAM provides the identity foundation, SoD delivers risk control, and Zero Trust binds them together into a cohesive, resilient security architecture.

REFERENCES

Executive Order No. 14028. (2021, May 12). *Improving the nation's cybersecurity*. The White House.

Government Accountability Office. (2014). *Standards for internal control in the federal government* (GAO-14-704G) [Green Book]. U.S. Government Publishing Office.

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.

National Institute of Standards and Technology. (2019). *Guide to attribute-based access control (ABAC) definition and considerations* (NIST Special Publication 800-162). U.S. Department of Commerce.

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53, Rev. 5). U.S. Department of Commerce.

National Institute of Standards and Technology. (2020). *Zero trust architecture* (NIST Special Publication 800-207). U.S. Department of Commerce.

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)*. U.S. Department of Commerce.

National Institute of Standards and Technology. (2025). *Digital identity guidelines* (NIST Special Publication 800-63-4). U.S. Department of Commerce.

Office of Management and Budget. (2016). *Management's responsibility for enterprise risk management and internal control* (OMB Circular A-123).

Office of Management and Budget. (2022). *Moving the U.S. government toward Zero Trust cybersecurity principles* (OMB Memorandum M-22-09).

About Electrosoft

Electrosoft is a cybersecurity, digital engineering, and intelligent automation firm delivering secure, scalable solutions for federal agencies. With 25 years of experience, the award-winning company combines deep mission expertise with modern engineering practices to help agencies operate securely, modernize with confidence, and accelerate operational performance. Electrosoft is headquartered in Reston, Virginia. www.electrosoft-inc.com.

About the Author
Mythili Arun, PMP, is an Electrosoft program manager serving in our Defense Operations division.