A Practical SAP Security Roadmap for UAE and Saudi Arabia

SAP holds transactions that keep an enterprise operating, including payments, procurement, payroll, inventory and asset maintenance. A compromised account or unauthorised change can create financial, operational and regulatory problems at the same time.

SAP security supports compliance by controlling access to business processes, limiting what each user can do and recording their activity. These controls help UAE and Saudi organizations meet the governance, monitoring, resilience and audit requirements established by the UAE Information Assurance Standard and Saudi NCA ECC.

The challenge is visibility. Periodic role reviews improve **audit readiness**, but it cannot show a SOC what's happening inside the **SAP landscape**. UAE IA and the **NCA Essential Cybersecurity Controls** require security to operate as part of **enterprise cybersecurity**, with evidence that controls remain effective between audits.

SAP powers mission-critical enterprise operations and regulatory compliance in the UAE and Saudi Arabia, but because static audits lack real-time visibility, organizations must integrate continuous, real-time SAP monitoring into their broader cybersecurity framework to meet strict national standards.

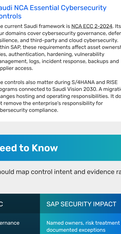
What Is SAP Security and Why Does It Matter?

SAP security combines governance, technical controls and operational processes to protect SAP identities, authorizations, transactions, configurations, interfaces, custom code and business data against unauthorized access, change, disclosure and disruption.

Effective ERP security covers several connected layers. Identity and access management verifies the user. SAP authorization determines which transactions and data that user can access. Segregation of Duties (SoD) prevents one person from controlling incompatible stages of a process, such as creating a supplier and approving its payment.

Security teams must also manage privileged access. SAP Security Notes, custom code, RFC connections, configuration baselines and audit logs. These controls protect business-critical systems against misuse by an attacker, employee, contractor or compromised account.

This distinction matters for SAP compliance. A clean role design may satisfy one access requirement, but it cannot identify an exploited vulnerability or suspicious transaction. SAP security and controls must cover prevention, detection, response and recovery.



How UAE IA and Saudi NCA ECC Apply to SAP Environments

Recent evidence shows why configuration and access deserve attention. The UAE Cyber Security Council reported in January 2025 that incorrect configurations accounted for 27% of the cyber incidents in its breakdown.

UAE Information Assurance Standard

The current UAE Information Assurance Standard is Version 2.1, issued in November 2025 by the UAE Cyber Security Council. The market still uses NESA compliance as shorthand because NESA issued the earlier standard.

UAE IA applies to federal authorities and relevant government and critical infrastructure entities. Its management controls address strategy, SAP governance, risk and compliance. Technical families cover assets, operations, networks, identity, third parties, system development, incidents and continuity. Each becomes relevant when SAP supports an in-scope process.

Saudi NCA Essential Cybersecurity Controls

The current Saudi framework is NCA ECC 2-2024. Its four domains cover cybersecurity governance, defense, resilience, and third-party and cloud cybersecurity. Within SAP, these requirements affect asset ownership, roles, authentication, hardening, vulnerability management, logs, incident response, backups and supplier access.

The controls also matter during S/4HANA and RISE programs connected to Saudi Vision 2030. A migration changes hosting and operating responsibilities. It does not remove the enterprise's responsibility for cybersecurity compliance.

UAE IA vs NCA ECC: What SAP Teams Need to Know

The frameworks organize requirements differently. SAP teams should map control intent and evidence rather than expect a one-to-one compliance comparison.

SECURITY AREA	UAE IA STANDARD	SAUDI NCA ECC	SAP SECURITY IMPACT
Governance and risk	Strategy, risk and compliance families	Cybersecurity Governance	Named owners, risk treatment and documented exceptions
Identity and access	Identity and Access Management	Cybersecurity Defense	Roles, MFA, user lifecycle and recertification
Secure operations	Operations and system-development controls	Cybersecurity Defense	Patching, hardening, custom code and change control
Logging and incidents	Operations and Incident Management	Cybersecurity Defense	SAP-aware alerts, investigation records and response
Resilience	Information Systems Continuity	Cybersecurity Resilience	Tested backups, recovery procedures and process availability
Cloud and suppliers	Third-Party Security	Third-Party and Cloud Cybersecurity	RISE responsibilities, remote access and service assurance

This is a working governance framework for control owners. Formal enterprise compliance still depends on scope, risk assessment, implementation evidence and the requirements of the relevant authority.

Six SAP Security Risks That Create Compliance Gaps

1. **Excessive privileges**
   Broad or accumulated roles weaken least privilege and can let users alter sensitive transactions or data.
2. **SoD conflicts**
   A user who can initiate and approve the same process can bypass checks designed to prevent error and fraud.
3. **Uncontrolled emergency access**
   Shared or poorly reviewed Firefighter IDs make privileged actions difficult to attribute.
4. **Unpatched vulnerabilities and insecure code**
   Delayed SAP Security Notes, unsafe custom ABAP and weak parameters can leave exploitable paths open.
5. **Insecure RFC connections**
   Trusted interfaces can enable unauthorized execution or movement between connected systems.
6. **Weak audit visibility**
   Logs without SAP context leave SOC analysts unable to distinguish a routine transaction from privilege abuse, an insider threat or attack activity.

Each weakness can affect operational continuity and audit results. Ransomware or destructive ERP access can interrupt purchasing, finance, production or logistics.

Essential SAP Security Controls for UAE IA and NCA ECC Alignment

Identity, Access and SoD

Apply least privilege to roles and remove access when employees or contractors change responsibilities. Enforce MFA for remote, administrative and high-risk access. Run SoD analysis before assigning a role, then recertify access against current duties.

Privileged and Emergency Access

Use named administrator accounts and time-bound elevation. Emergency Access Management should record the request, approval, activity and post-use review for each Firefighter session. Shared permanent administrator access prevents reliable accountability.

Hardening and Vulnerability Management

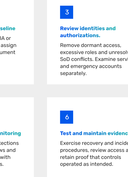
Maintain an approved baseline for SAP parameters, services and interfaces. Review SAP Security Notes, prioritize vulnerabilities by exposure and business impact, and test patches before production deployment. Scan custom code, restrict RFC destinations, encrypt data in transit and validate backups.

Logging, Detection and Response

Enable logs covering users, transactions, configuration changes and privileged activity. Retain them according to policy and feed actionable events into the SOC. Response playbooks should identify who can contain an account, reverse a change, preserve evidence and involve the process owner.

10-control checklist

- Maintain an inventory of SAP systems, interfaces and owners.
- Enforce MFA and risk-based access.
- Review roles, SoD conflicts and dormant accounts.
- Control and review privileged sessions.
- Apply SAP Security Notes through a risk-based patch process.
- Scan custom code and monitor transports.
- Harden SAP parameters and RFC connections.
- Encrypt sensitive connections and stored data where required.
- Send contextual SAP events to the SOC.
- Test backups, recovery and incident playbooks.



SAP GRC Access Control supports role governance, SoD analysis, access certification and Emergency Access Management. It contributes to SAP risk management and audit evidence. It does not provide the vulnerability detection, security analytics or incident operations required across the wider SAP environment.

CONTROL GROUP	UAE IA ALIGNMENT	NCA ECC ALIGNMENT	EVIDENCE
Identity and privilege	Identity and Access Management	Cybersecurity Defense	Approvals, role reviews and access records
Hardening and patching	Operations Management	Cybersecurity Defense	Baselines, scan results and patch records
Monitoring and response	Operations and Incident Management	Cybersecurity Defense	Alerts, cases and response logs
Recovery and suppliers	Continuity and Third-Party Security	Resilience and Third-Party/Cloud	Test results, contracts and responsibility records

A Six-Step SAP Security Roadmap

1. **Assess the SAP landscape**
   Record ECC, S/4HANA, RISE, custom code, interfaces, sensitive data and the processes each system supports.
2. **Set the compliance baseline**
   Identify applicable UAE IA or NCA ECC requirements, assign control owners and document accepted risks.
3. **Review identities and authorizations.**
   Remove dormant access, excessive roles and unresolved SoD conflicts. Examine service and emergency accounts separately.
4. **Implement security controls**
   Remediate exposed vulnerabilities, unsafe configurations, insecure RFC connections and gaps in encryption or backup.
5. **Enable continuous monitoring**
   Connect SAP-aware detections to existing SOC workflows and define escalation paths with SAP and process owners.
6. **Test and maintain evidence**
   Exercise recovery and incident procedures, review access and retain proof that controls operated as intended.

A practical **cybersecurity roadmap** uses different cadences. Monitor security events continuously. Review privileged access and SoD at least quarterly. Perform a **maturity assessment** annually and after major migrations, acquisitions or architecture changes. Apply **Zero Trust** principles by verifying identity, device, privilege and transaction context when risk warrants it.

How Security Priorities Change Across Regulated Sectors

GOVERNMENT
Protect citizen services and restrict administrative access across connected enterprise applications

BFSI AND HEALTHCARE
Preserve transaction or record integrity while producing evidence of who viewed, approved or changed sensitive data.

OIL, GAS AND UTILITIES
Map SAP dependencies that could affect maintenance, supply, assets and critical operations.

MANUFACTURING AND TRANSPORT
Secure supplier, inventory, production and logistics interfaces without disrupting availability.

The framework remains the baseline. Process criticality determines which SAP cyber security controls receive priority.

How Paramount Assure Supports SAP Security Operations

Paramount's SAP security consulting includes compliance assessments of configurations, patching, custom code, logging, SoD, emergency users, change control and RFC access. The resulting risk view helps organizations decide which gaps require remediation and which SAP events belong in the SOC.

This model supports ECC, S/4HANA, RISE and hybrid environments. Organizations can begin with an SAP SOC assessment before selecting the required managed security services.

Request an SAP SOC assessment to identify the access, configuration and monitoring gaps affecting your UAE IA or NCA ECC alignment.