Arcon

Kingdom of Saudi Arabia Compliance . OT CYBERSECURITY

Operational Technology Cybersecurity Controls

A compliance guide mapping ARCON Privileged Access Management to the NCA's OTCC requirements for industrial and, ICS environment.

FRAMEWORK	ISSUED BY	DOMAIN FOCUS	CLASSIFICATION
NCA OTCC Ecc-1:2018 baseline	**National Cybersecurity Authority**	**Privileged Access Management**	**Public**

PREDICT PROTECT PREVENT

CONCLUSION

ARCON Privileged Access Management enables SRM leaders to:

- ✓ Comply with OTCC guidelines pertaining to Privileged Identity Management
- ✓ Ensure robust privileged identity management environment enterprise-wide
- ✓ Mitigate the chances of data breach incidents and IT security vulnerabilities
- ✓ Meeting the demands of advanced PAM use cases as highlighted in OTCC compliance guidelines

CONTENTS

Inside this brief

Arcon

Saudi Arabia's cybersecurity landscape

Saudi Arabia's current IT security scenario combines strong national cybersecurity maturity with a high and rising threat level. The Kingdom has built a robust, regulator-led cyber posture through the **National Cybersecurity Authority (NCA)**, mandatory frameworks like ECC (Essential Cybersecurity Controls) and OTCC (Operational Technology Cybersecurity Controls), and major investment aligned to Vision 2030. This has improved baseline controls, compliance culture, and national readiness, with KSA consistently ranking among global leaders in cybersecurity and digital government.

At the same time, Saudi Arabia is a prime target due to its geopolitical role, energy sector importance, and rapid digitization. Threat trends show persistent ransomware campaigns, credential and data leaks on the dark web, and periodic state-linked or hacktivist activity. Critical infrastructure, industrial/ OT environments, government, finance, and large digital-service organizations face the greatest pressure. Rapid cloud adoption and expansion of smart city/ mega-projects also increase attack surfaces, making identity security, privileged access management, continuous monitoring, and third-party risk control key priorities.

> Saudi Arabia has strong defenses and regulations but remains one of the most targeted and fast-expanding cyber environments globally.

Arcon

THE FRAMEWORK

What OTCC compliance means

OTCC regulatory compliance refers to meeting the Saudi National Cybersecurity Authority's Operational Technology Cybersecurity Controls requirements for industrial/ ICS (Industrial Control Systems) environments.

What is it: OTCC is a national OT/ICS-specific control framework issued by Saudi Arabia's NCA. It is designed to provide detailed cybersecurity controls for operational technology and industrial control systems, especially in critical facilities.

How compliance works (dependency on ECC): OTCC is an extension of the **Essential Cybersecurity Controls (ECC-1:2018).** Organizations must first comply with ECC and then implement the additional OTCC controls to be considered OTCC-compliant

Alignment to global standards: OTCC compliance is structured so organizations can map their implementation to leading OT/ICS standards such as IEC/ISA 62443, NIST CSF, NIST SP 800-53/800-82, NERC CIP, and others. This makes OTCC a regulator-backed "local wrapper" over internationally recognized practice.

Risk-based applicability: OTCC uses facility criticality levels (L1–L3). The higher the criticality, the more controls are mandatory. Compliance is achieved by identifying the facility level and applying all controls required for that level.

Regulatory precedence: If there is any conflict between OTCC and other referenced standards, **OTCC takes precedence** for compliance purposes in Saudi Arabia.

CONTROL MAPPING . PAM-ADJACENT

Secure Remote Access, Segmentation & Network Gatekeeping (PAM-adjacent)

OTCC emphasizes strict segmentation and controlled connections, especially remote/third-party/admin access, which a PAM gateway/broker typically enforces.

CONTROL	SCOPE	MAPPED STANDARDS
2-4	Network Security Management - controls 2 - 4-1-1 -> 2-4-1-16 include segmentation, secure connections to/from corporate and external networks, and remote - access protections.	NIST AC - 17 NIST SC - 7 IEC 62443 SR 5.1 / 5.2
ECC OTCC	5-1-3-1 / 5-1-3-2 (from ECC Domain 5 mapping) require strict physical/virtual segmentation for OT⊠IT and OT⊠external/Internet/remote access links; these are implemented through controlled access paths and jump/bastion/PAM brokers.	

ARCON PAM features that can map OTCC compliance:

- PAM jump server / OT access broker (single controlled path into OT zones).
- Network-level allowlisting is tied to privileged sessions.
- Time-bound access for vendors/engineers through PAM.
- Protocol proxying (RDP/SSH/industrial protocols) with inspection.
- Zone-based access policies aligned to OT segmentation requirements.

Aarcon

CONTROL MAPPING . DIRECT PAM SCOPE

Core Identity & Access Management (direct PAM scope)

The OTCC has a dedicated subdomain **2-2 Identity and Access Management,** under Cybersecurity Defense. This is your primary PAM anchor.

CONTROL	SCOPE	MAPPED STANDARDS
2-2-1	Sub controls 2-2-1-1 through 2-2-1-11 covers identity lifecycle, account management, authentication, authorization, and access enforcement in OT/ICS.	NIST PR.AC-1/3/7, NIST 800-53 AC-2/3/11/12, and IEC 62443 SR 1.x / SR 2.x / SR 5.2, which are classic access control + privileged access foundations.
2-2-2	Continuing IAM requirements OT/ICS environments.	NIST PR.AC-1ations. IEC 62443 SR 1.2

ARCON PAM features that can claim compliance coverage for:

- Centralized privileged account inventory and ownership.
- Joiner-Mover-Leaver provisioning/deprovisioning for OT identities.
- Strong authentication / MFA for privileged users.
- Role-based and policy-based access to OT assets.
- Least privilege + separation of duties for control system operations.
- Password/secret standards for privileged credentials.
- Session access enforcement (allow/deny based on entitlement).

Arcon

CONTROL MAPPING . EVIDENCE & ACCOUNTABILITY

Privileged Session Monitoring & Audit Trails

PAM compliance papers usually need recording, monitoring, and non-repudiation for privileged activity. OTCC supports that through log/monitoring and periodic review controls.

CONTROL	SCOPE	MAPPED STANDARDS
2-11	Event Logs & Monitoring Management – 2-11-1 and its sub-controls (2-11-1-1 through 2-11-1-10) cover log activation, continuous monitoring, and security event capture.	NIST PR. PT-1 NIST DE.AE / DE.CM 800-53 AU
ECC LINK	Periodical Cybersecurity Review & Audit - 1-6-1 / 1-6-2 require periodic audit and review of controls, needed for PAM evidence cycles.	NIST ID.GV 800-53 CA

ARCON PAM features that can map OTCC compliance:

- **Full privileged session recording (video/keystrokes/commands).**
- **Real-time session monitoring and alerting**
- **Immutable audit logs for privileged actions.**
- **Automated compliance reporting for OT access**
- **Privileged activity analytics (anomaly detection).**

CONTROL MAPPING . FOUNDATION

Secure Configuration/Hardening that Locks Down Privileged Paths

While not “IAM controls” per se, OTCC requires hardening and secure configuration of systems that PAM relies on - endpoints, jump hosts, admin interfaces.

CONTROL	SCOPE	MAPPED STANDARDS
2-3	System & Processing Facilities Protection – Controls 2-3-1-1 through 2-3-1-13 and 2-3-2 cover secure configuration, administrative interface handling, malware protection, and removable media restrictions.	NIST PR. AC NIST PR.PT
ECC LINK	5-1-3-7 — periodic review and secure configuration/hardening of industrial systems/devices. 5-1-3-5 — strict limitation on external storage (reduces privileged misuse of vectors).	

ARCON PAM features that can map OTCC compliance:

- **Controlled elevation** on OT endpoints (no local admin sprawl).
- **Application allow listing tied to privileged roles.**
- **Device posture checks before the privileged session starts.**

CONTROL MAPPING . SUPPLY CHAIN

Third-Party / Vendor Privileged Access Governance

OT environments heavily depend on vendors; OTCC has a whole domain for third-party cybersecurity, which PAM commonly enables.

CONTROL	SCOPE	MAPPED STANDARDS
4-1	Third-Party Cybersecurity – Control 4-1-1 and its sub-controls (4-1-1-1 through 4-1-1-4), together with Control 4-1-2, govern supplier access.	NIST ID.SC NIST SA-12 OT supplier risk

ARCON PAM features that can map OTCC compliance:

- **Vendors access workflows** (approval, just-in-time, time-boxed).
- **Contractor identity federation** into PAM without sharing plant credentials.
- **Per-vendor session recording and evidence packs.**

Arcon

CONTROL MAPPING . SUPPLY CHAIN

What to de-prioritize/ exclude for a PAM-only mapping

For a PAM + secure access control compliance paper, you can largely exclude these OTCC areas unless you want broader GRC coverage:

2-1	**Asset Management** Useful context, but not PAM core.	2-6 . 2-7	**Data & Information Protection, Cryptography** Tangential to PAM unless you cover secret encryption.
2-8 . 9 . 10	**Backup, Vuln Mgmt & Pen Testing** Operational security, not access control.	2-13	**Physical Security** Only overlap is physical console access.
3-1	**BCM / Resilience** Not PAM-specific	1-7 . 1-8	**Governance, HR & Awareness** Supporting controls, not feature mapping.

EXHIBIT . AT A GLANCE

ARCON compatibility chart

OTCC REQUIREMENT	ARCON PAM CAPABILITY
MFA for privileged access	MFA integration
Secure OT remote access	Secure gateways
Session recording	Video + text logging
Unique user accountability	Named accounts
Password complexity & rotation	Vault
Emergency access management	Break-glass workflows
Vendor access control	Third-party access governance
Access approvals	Workflow engine
Audit logs retention	Immutable logs
SOC integration	Syslog/SIEM connectors
Command control	SSH command filtering
Time-based access	JIT access


arcon