Find out how ARCON | Privileged Access Management elevates security controls and helps to comply with the Telecommunications security Act (TSA)

Table of Content

The Context

Organizations that heavily leverage technology, especially the likes of the telecommunication industry, are increasingly facing challenges due to technological complexities and associated IT infrastructure risks. The privileged identities are more vulnerable to such risks.

The telecommunication industry has moved towards the Fifth Generation (5G) wireless technology. So, the infrastructure requirement along with the number and types of telecommunication equipment are huge for 5G core telco networks. Today's modern-day core telco networks teams invariably manage operations in a highly distributed IT environment. The workforce is spread across several locations wherein remote and third-party access is frequent, including privileged access.

Therefore, the threat surface for core telco networks is fairly wide that transcends traditional datacenter set-up. Data integrity, Data privacy, and Data Confidentiality could be jeopardized if hundreds of thousands of telecom equipment with privileged access to confidential information are vulnerable to unauthorized access. ARCON | Privileged Access Management (PAM) solution provides core telco networks with a unified governance framework to manage, protect and monitor privileged identities.

Cybersecurity Challenges in Telecom Industry

The telecom industry faces several significant cybersecurity challenges, including:

- **Supply Chain Vulnerabilities:** Telecom operators often rely on third-party vendors for infrastructure. Any vulnerabilities within these external entities can compromise the entire supply chain.
- **Distributed Denial-of-Service (DDoS) Attacks:** These attacks can render services inaccessible, causing major disruptions for millions of users who depend on continuous connectivity.
- **Phishing:** Phishing emails are common gateways for ransomware attacks, posing a significant threat to telecom companies.
- **Insider Threats:** Employees with access to sensitive information can intentionally or unintentionally cause security breaches.
- **Legacy Technology:** Many telecom companies still use outdated systems that are more vulnerable to cyberattacks.
- **Quantum Computing:** The advent of quantum computing poses a future threat as it has the potential to break widely used cryptographic algorithms.

Addressing these challenges requires robust cybersecurity measures, continuous monitoring, and updating of security protocols to protect sensitive data and ensure service continuity.

Telecommunications Security Act (TSA): Securing Telecom Networks and Enhancing Privacy Controls

The Telecommunications (Security) Act 2021, enacted in the United Kingdom, is designed to enhance the security and resilience of telecommunications networks. It was introduced following the UK Telecoms Supply Chain Review Report in 2019, which highlighted the need for a stronger security framework due to the increasing threats in cybersecurity, especially with the rise of 5G and full-fiber networks.

Key features of the TSA include:

- **Stronger Security Duties:** Telecom providers must implement measures to identify and defend against cyber threats and prepare for future risks. This includes taking swift action to limit, remedy, and mitigate damage from security compromises.
- **General Security Duties:** Providers are required to inform those affected by security compromises, notify OFCOM (the UK communications regulator), and reduce risks.
- **Supply Chain Management:** Enhanced risk management processes for third-party suppliers, ensuring better visibility and updated contractual arrangements.

The Act aims to ensure that telecom networks remain secure and resilient against evolving cyber threats, thereby protecting the integrity and functionality of these critical infrastructures.

What are the core objectives of TSA?

The Telecommunications (Security) Act 2021 has several core objectives aimed at enhancing the security and resilience of telecommunications networks in the UK. Here are the key objectives:

1. **Strengthening Security Measures**

Telecom providers are required to implement robust security measures to protect their networks from cyber threats. This includes identifying potential risks, defending against attacks, and preparing for future threats.

2. **Swift Response to Security Compromises**

The Act mandates that providers take immediate action to limit, remedy, and mitigate the damage caused by any security compromise. This ensures that any breach is quickly contained, and its impact minimized.

3. **Supply Chain Security**

Providers must enhance their risk management processes for third-party suppliers. This involves ensuring better visibility and control over the supply chain and updating contractual arrangements to include security requirements.

4. **Regulatory Compliance and Reporting**

Telecom providers are required to inform OFCOM (the UK communications regulator) and those affected by security compromises as soon as reasonably practicable. This ensures transparency and accountability in handling security incidents.

5. **Ongoing Risk Management**

The Act emphasizes the need for continuous risk assessment and management. Providers must regularly review and update their security measures to address evolving threats and vulnerabilities.

These objectives aim to create a more secure and resilient telecommunications infrastructure, capable of withstanding the increasing threats in the digital age.

Role of Privileged Access Management (PAM) in complying with TSA

Privileged Access Management (PAM) plays a crucial role in helping organizations comply with the Telecommunications Security Act (TSA). Here are some ways through which PAM contributes to compliance:

- **Access Control:** PAM ensures that only authorized personnel have access to critical systems and data. By managing and monitoring privileged accounts, it helps prevent unauthorized access, which is a core requirement of the TSA.
- **Risk Mitigation:** PAM solutions help identify and mitigate risks associated with privileged access. This includes implementing strong authentication methods, session monitoring, and automated workflows to manage access requests.
- **Incident Response:** Unauthorized access attempts, irregular logins, account takeovers – in short, any abnormal behavior patterns of identities face enormous security threats. ARCON | PAM embedded with Identity Threat Detection and Response (ITDR) capability helps to build a proactive security posture.
- **Monitoring and Auditing:** Continuous monitoring of privileged user activities and maintaining detailed audit trails are critical for compliance. PAM solutions offer comprehensive logging and reporting capabilities, making it easier to demonstrate compliance during audits.
- **Reporting:** PAM simplifies the process of mandatory reporting of cybersecurity incidents and vulnerabilities. Detailed logs and reports generated by PAM solutions help organizations meet the TSA's reporting requirements.

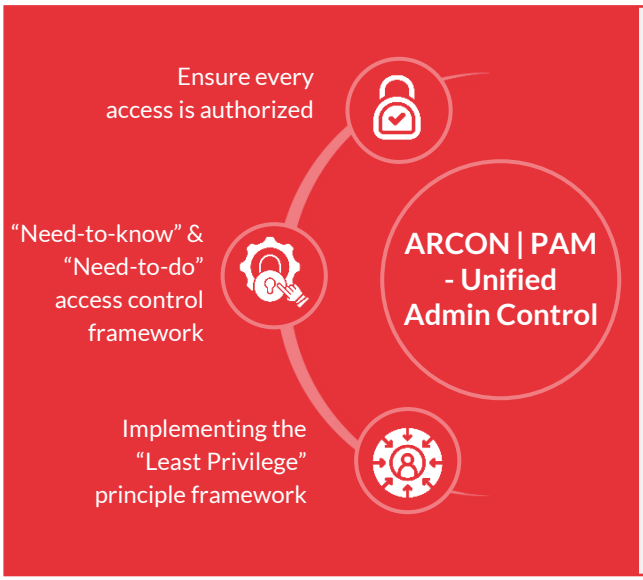
By implementing a robust PAM solution, telecommunications providers can ensure they meet the stringent security and compliance requirements set forth by the TSA, thereby protecting their critical infrastructure from emerging cyber threats.

TSA Checklist and how ARCON's Privileged Access Management solution addresses the requirements

TSA Requirements

(1) The provider of a public electronic communications network or a public electronic communications service must take such measures as are appropriate and proportionate for the purposes of—

(a) identifying the risks of security compromises occurring;
(b) reducing the risks of security compromises occurring;

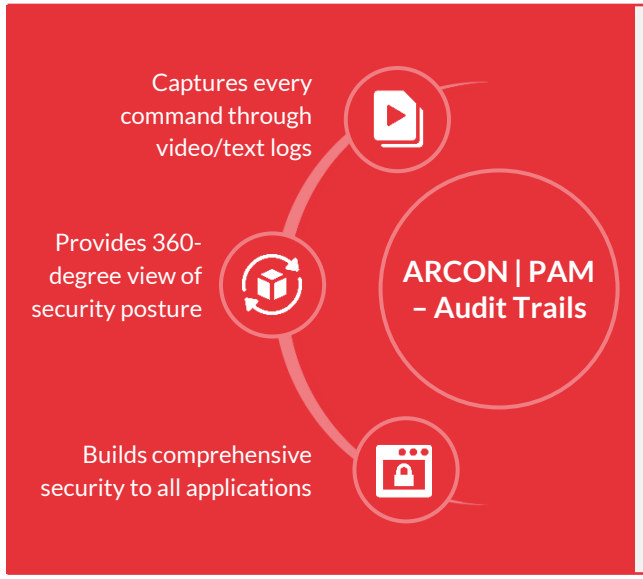


(2) In this Chapter "security compromise", in relation to a public electronic communications network or a public electronic communications service, means—

(1) (b)any unauthorized access to, interference with or exploitation of the network or service or anything that enables such access, interference or exploitation;

(3) A monitoring direction may make provision about—
(a)the form of a report;
(b)the content of a report.

(4) (a) A security report must include —
(a)information about the extent to which providers of public electronic communications networks and public electronic communications services have complied during the reporting period with the duties imposed on them by or under sections 105A to 105D, 105I to 105K, 105N(2)(a) and 105O



(4) A monitoring direction may require a report to include—

(a) OFCOM's analysis of information gathered by them;
(b) an explanation of their analysis.

Conclusion

By deploying ARCON | Privileged Access Management, telecom service providers can –

- Identify, assess, and mitigate IT operational and infrastructure risks emanating from unauthorized privileged access
- Get detailed analysis of the privileged access reports to assess risks and remain audit-ready
- Build a comprehensive security posture

about ARCON

ARCON is a leading Information Risk Management solutions provider specializing in Privileged Access Management and Continuous Risk Assessment solutions.

ARCON Privileged Access Management (PAM) is a leading global product and a robust solution that mitigates risks arising out of privilege identity and access management.

Connect with us