المركـز الوطنـي للأمـن السيبرانـي
National Cyber Security Center

2025-2028

Jordan Energy Sector Cyber Security Strategy

Cyber resilient, secure and trusted, enabling digital transformation and smart technologies

March 2025

Executive Summary

The Kingdom of Jordan recognises the critical importance of securing its energy sector from escalating cyber threats. This strategy outlines an ambitious plan to enhance the sector's cyber resilience by 2028, ensuring a secure digital transformation and safeguarding national and economic security. Aligned with the National Cyber Security Strategy (2025–2028), the National Cyber Security Framework 2024 (JNCSF), and the National Energy Strategy (2020–2030), it provides a roadmap for addressing vulnerabilities arising from legacy systems, limited cyber security skills, and emerging technological threats.

The strategy identifies significant challenges, including a lack of sector-specific regulation, economic constraints, technological complexities from the increasing convergence of Information Technology (IT) and Operational Technology (OT) systems, and skill shortages. It also highlights the sector's unique vulnerabilities to advanced threats, such as those targeting interconnected smart grids and Internet of Things (IoT) devices.

To mitigate these risks, this strategy focuses on three core objectives:

1. **Strengthening governance and policy:** Establishing robust governance frameworks, enforcing high standards across the sector, and ensuring clear roles and responsibilities. This includes maintaining a centralised asset register, conducting regular risk assessments, and embedding cyber security into corporate policies.
2. **Establishing security operations capabilities:** Energy organisations will develop SOCs, and build foundational incident response and cyber threat intelligence capabilities. A sector-wide Energy Cyber Emergency Response Team (En-CERT) and an Early Warning System (EWS) will be established under the Energy and Minerals Regulatory Commission (EMRC) and the National Cyber Security Centre of Jordan (NCSC-JO) respectively to enhance incident response and threat detection.
3. **Developing cyber security skills and culture:** Companies will implement mandatory annual training, advanced role-specific programmes, and board-level cyber security ownership.

Collaboration is a cornerstone of this strategy. NCSC-JO, alongside EMRC and the Ministry of Energy and Mineral Resources (MEMR), will work closely with public and private stakeholders to implement the strategic objectives and promote information sharing, joint exercises, and coordinated responses.

This strategy is not merely an endpoint, but a living framework for continuous improvement in the Kingdom's cyber resilience. It will be tracked and updated as Jordan moves along its journey towards a cyber secure and resilient future and will serve as a model for upcoming cyber security strategies across other critical sectors.

Content

Context

The Kingdom of Jordan is committed to ensuring the cyber security of its energy sector. Reliable energy is vital to national resilience, long-term security and prosperity – including by powering households and businesses, fuelling the transportation industry, and underpinning essential services.

The Kingdom's energy sector remains – however – vulnerable to a range of serious cyber threats. This is partly due to a current lack of sector-specific regulation and cyber security skills in the workforce, as well as the integration of new digital technologies into often legacy energy systems. Successful attacks against Jordan's energy operators by hostile nation states or financially motivated cyber criminals could result in energy supply disruptions that pose serious risks to everyday life.

Action is required to build the sector's cyber security capabilities and establish strong risk management frameworks to ensure that Jordan's energy infrastructure is resilient to both current and future cyber threats. As a key component of Jordan's Critical National Infrastructure (CNI), the energy sector must ensure it can operate securely and continuously in the face of escalating cyber threats. Enhancing the energy sector's capability to prevent, detect and respond to threats targeting its infrastructure will help to make the sector and Jordan as a whole a harder target, build trust across its citizens, and provide space for Jordan to achieve its wider economic goals.

Responding to these needs, **this strategy sets out an ambitious plan to sustainably enhance the cyber resilience in the Kingdom's energy sector by 2028, ensuring its secure digital transformation**[1] **and safeguarding national and economic security.** In striving for this aim, this strategy is closely aligned with the National Cyber Security Strategy (2025-2028), Jordan's National Cyber Security Framework 2024 (JNCSF – see Annex B), and the overarching National Energy Strategy 2020-2030. This strategy also supports Jordan's Economic Modernisation Vision by contributing to the broader goal of fostering secure, sustainable economic growth.[2]

This strategy's focus, including Vision, Mission, and Strategic Objectives, has been informed by a number of in-depth consultations with representatives from EMRC, MEMR, NCSC-JO, and key energy sector operators (the "companies") responsible for power generation, storage, and distribution across Jordan. This ensured that the strategy **reflects the collective expertise and priorities of the energy sector,** while **addressing its unique challenges and aligning with national economic and strategic goals**.

[1] The Government of Jordan's digital transformation ambitions, set out in Jordan Digital Transformation Strategy 2020, includes embracing a range of modern technologies including 5G, Internet of Things, and artificial intelligence in digital government services.

[2] A Comprehensive National Vision to Support and Develop the National Economy https://jordanvision.jo/en

Stakeholders

The success of this strategy is contingent on strong collaborative efforts among key stakeholders, including:

- **Companies** across the energy industry that will act on this strategy and serve as their own first line of defence.[3] This applies to public and private companies including in electricity, renewables, oil, and gas, working in generation and transportation to distribution, refining, and storage of energy;

- **NCSC-JO** is the regulator for cyber security in Jordan and central co-ordinator for cyber security initiatives on the national level; it will lead on the implementation of the strategy, and audit and monitor compliance with the strategy across the energy sector to ensure alignment with established policies and standards;

- **EMRC** is the regulatory and supervisory body responsible for overseeing the operational implementation of the strategy on behalf of NCSC-JO. It will coordinate closely with NCSC-JO to help companies in the energy sector understand and adopt the Strategy and work towards achieving the Strategic Objectives. EMRC will also be responsible for tracking the fulfilment of the benchmarks outlined in the Strategy Implementation Roadmap,[4] monitoring companies' progress towards improving their cyber resilience and implementing the strategy.

- **MEMR** is responsible for formulating and approving policies in the energy sector, and will ensure alignment with the overarching Energy Sector Strategy 2020-2030.

[3] As in line with Jordan's National Cyber Security Framework 2024.
[4] Outlined in Annex A.

Challenges and Opportunities

While this strategy is necessitated by a range of serious and urgent challenges, it is equally informed by opportunities and facilitating factors that support its implementation. The table below first outlines current positive circumstances that enable progress, followed by the key challenges that must be addressed to strengthen the cyber resilience of Jordan's energy sector.[5] **MEMR** is responsible for formulating and approving policies in the energy sector, and will ensure alignment with the overarching Energy Sector Strategy 2020-2030.

Political • Significant national progress in cyber security efforts through JO-CERT, NCSC-JO, and the National Cyber Security Strategy (2024-2028). • Policy gaps and inconsistent practices in the energy sector increase vulnerability to cyber threats. • Proximity to regional conflicts heightens the need for robust defensive measures.	**Technological** • Digital transformation efforts and active adoption of advanced technologies like smart grids can support cyber resilience efforts.[6] • OT systems typically were not designed with security in mind; their convergence with IT introduces critical vulnerabilities. • Emerging threats like Artificial Intelligence-driven attacks, supply chain risks, and quantum computing demand proactive defences such as quantum-resistant encryption and AI-based detection. • Patchy incident response frameworks across the sector and limited advanced threat detection capabilities leave the sector ill-prepared for serious incidents.
Economic • Strong national and foreign investment in energy infrastructure supports cyber security potential. • Budget constraints, reliance on foreign aid, and weak enforcement may hinder progress. • Limited board-level awareness and insufficient budget allocation leave assets vulnerable.	**Environmental** • Commitment to renewable energy offers opportunities to embed security into new infrastructure from the onset. • Climate-related risks (e.g., extreme heat, flooding, natural disasters) threaten infrastructure and operational stability. • Inconsistent disaster recovery and business continuity plans, and a lack of physical controls such as flood protection measures, exacerbate risks.
Social • Growing awareness and governmental focus on securing energy infrastructure. • Workforce and skills shortages, particularly in OT security, are critical concerns. • Universities and capacity-building initiatives are key to addressing talent gaps.	**Legal**[7] • Regulatory frameworks like National Cyber Security Framework (JNCSF) are enhancing cyber resilience standards. • Gaps in laws governing critical national energy infrastructure and limited resources for audits remain challenges. • Alignment with international standards (e.g., GDPR, ISO) can improve security and cross-border co-operation.

[5] See Annex C: The Challenge: Detailed analysis.
[6] As outlined in the overarching Energy Sector Strategy 2020-2030.
[7] See Annex B: Alignment with national cyber regulation.

The Threat

The Kingdom of Jordan continues to be a target for a range of cyber threat actors, with NCSC-JO reporting 2,455 cyber incidents in 2023—a staggering 80% increase from 2022. Government networks and critical national infrastructure, particularly in the energy sector, are primary targets**. Disruptions to energy networks could severely impact operations and Jordanian citizens' lives** - underscoring the need for an integrated and coordinated Energy Sector cyber security strategy.

The energy sector worldwide has faced a significant rise in targeting. This is primarily driven by three key factors:

- **Aging energy infrastructure**, including legacy technologies that were not built with cybersecurity in mind, remains vulnerable due to infrequent updates and long equipment lifespans.
- The **growing convergence of IT and OT** in energy networks introduces vulnerabilities as OT systems become more closely connected to enterprise networks and the internet. Threat actors can exploit these weaknesses to disrupt energy operations, and move from IT to OT systems - risking widespread outages and power supply interruptions for Jordanian citizens.
- The energy sector's **dependency on complex global supply chains** complicates the coordination of cybersecurity measures and Incident Response (IR), and make consistent security implementation challenging.

Significant threats to energy infrastructure arise from state-sponsored, criminal, and hacktivist cyber threat groups.

- **State-sponsored:** These groups engage in espionage and, at times, destructive attacks on OT systems like Industrial Control Systems (ICS), sometimes with severe consequences.
- **Cyber criminals**: Specifically ransomware attacks on energy systems may lead to financial losses and operational disruptions. Opportunistic targeting by criminals makes this an unpredictable and pervasive threat.
- **Hacktivists**: Ideologically driven actors may demonstrate the capacity to disrupt critical infrastructure extensively.

In addition, the sector faces a range of emerging cyber threats:

- The ongoing digital transformation and adoption of smart grids, IoT devices, and renewable energy sources[8] further expands the sector's attack surface.
- The integration of advanced technologies like Artificial Intelligence (AI) and Machine Learning (ML) introduces emerging threats, particularly through AI-driven malware capable of adapting to evade detection by traditional security tools. This is particularly dangerous for sectors like energy, where legacy OT systems often lack the flexibility to quickly adopt new cybersecurity measures, creating vulnerabilities that advanced threats can exploit. Quantum computing further threatens traditional encryption, requiring proactive investment in quantum-resistant solutions.

Given the range and scale of these threats, a strategic, coordinated approach is essential to safeguard the Kingdom's energy sector against emerging cyber risks. The following section outlines the strategic steps the Kingdom will take to strengthen cyber resilience and ensure robust defence mechanisms across the energy sector.

[8] As outlined in the overarching Energy Sector Strategy 2020-2030.

Vision and Mission

The strategy sets clear goals to transform the sector into a resilient, secure, and trusted part of Jordan's digital ecosystem. It is designed to be implemented over a four-year period (2025-2028), aligning with the National Cyber Security Strategy (2024-2028), Jordan's National Cyber Security Framework 2024, and the National Energy Sector Strategy 2020-2030. This timeframe allows for continuous adaptation to the evolving threat landscape, enabling the sector to build a more secure, resilient, and future-ready infrastructure.

This strategy's **vision** is that **by 2028 Jordan's energy sector will be cyber resilient, secure and trusted, enabling digital transformation and smart technologies.**

Achieving this vision will require commitment from all stakeholders, ensuring a seamless integration of cyber security measures across the sector and government.

To drive the improvements required, our **mission** is thus to **sustainably enhance the energy sector's cyber security infrastructure, expand our skilled cyber security workforce, and foster sector-wide collaboration to ensure a resilient energy network.**

Strategic Objectives

To achieve mission and vision, we will focus on delivering three Strategic Objectives that will address the most pressing cyber challenges faced by Jordan's energy sector:

1. **Strengthening governance and policy** – Establish high-level cyber security policies and frameworks with clear management decisions, identify critical assets, and thus ensure consistent standards and improved security across the energy sector. This will provide structure and direction to guide continuous cyber improvements.

2. **Establishing security operations capabilities** – Build security operations capabilities across the sector to enable individual and collective resilience. This will include conducting company-level technology gap analyses, developing individual SOCs, and establishing and exercising IR capabilities. Additionally, it involves implementing CTI and collaboration mechanisms between regulators, operators and local and international stakeholders to improve information sharing and third-party risk management.

3. **Developing cyber security skills and culture** – Underpinning these Strategic Objectives, promote continuous cyber security training and foster a culture of security awareness at all levels across the energy sector. This will strengthen capabilities now and in the future.

In the following sections, each Strategic Objective is structured into:

- **Aim –** clarifying the purpose and intent behind each Objective.

- **Operational Plan -** including high-level actions to drive measurable progress over the 4-year timeframe. **Annex A consolidates timelines and milestones across all Strategic Objectives** to enable measurable success of the strategy.

- **Responsibilities** - Outlining the key actors and their specific roles in implementing each action to ensure clear accountability.

1 Strengthen governance and policy

We will develop comprehensive policies and frameworks that drive common high standards for cyber security across Jordan's critical infrastructure. This strategy creates a framework for the energy sector to define roles and responsibilities and promote continuous improvement, creating a secure, resilient and compliant cyber security environment.

Aims

Working in partnership, NCSC-JO and EMRC will support individual companies in establishing high-level, well-defined cyber security governance policies and frameworks. These efforts will align with NCSC-JO's existing strategies and policies, such as the National Cyber Security Strategy 2024-2028 and Jordan's National Cyber Security Framework, the Jordan Critical Infrastructure Standard, and Jordan's National Energy Strategy 2020-2030. This ensures that companies across the energy sector adhere to a consistent and robust set of security standards that align with international best practices. Our objectives here seek to:

- Develop a governance structure that clearly outlines roles and responsibilities.
- Improve compliance with cyber security regulations, strengthening the overall security posture of the energy sector.

High-Level Operational Plan

Action 1: Establish clear roles, responsibilities, and governance structures across the energy sector.

To drive effective cyber governance and accountability, companies in the energy sector will establish clear roles and governance structures that align with operational needs and foster a joined-up approach to IT, OT, cyber, physical, and personnel security, to ensure a holistic approach. This includes defining and formalising key positions, such as Chief information Security Officers (CISOs), who will oversee coordination of all security functions. CISOs should report directly to senior executives and board-level budget holders to ensure alignment between security priorities, risk management, and investment decisions.

In alignment with the Jordanian National Cyber Security Framework, energy sector companies should establish an independent cyber security unit, separate from the overarching IT unit. This unit will be responsible for enforcing policies and ensuring consistent security coverage across IT and OT environments. Effective governance should prioritise balancing security investments with risk mitigation strategies, coordinating security functions, and conducting regular testing of systems and connections to validate resilience.

Furthermore, activities should include standardising documentation practices and implementing robust knowledge management processes to address inconsistencies across IT, OT, and cyber security domains. This will ensure uniformity in policy, procedures, and IR plans, thereby reducing gaps in understanding and improving cross-functional coordination.

Responsibilities:

- *Each individual energy sector company* should create a dedicated cyber security unit, as well as a dedicated security officer role (such as CISO) or an equivalent role at a senior level, responsible for overseeing information and cyber security. These officers should have clearly

defined, cross-departmental responsibilities. Companies must also develop governance structures that clearly articulate decision-making processes, reporting lines, and accountability mechanisms for cyber security management. This includes ensuring transparent, up-to-date knowledge management mechanisms that facilitate clear communication and regulatory compliance. This also includes the transparent documentation of organisational policies, security protocols, and IR plans. These should be regularly tested to ensure they are fit for purpose, identify gaps, and drive continuous improvement.

- *NCSC-JO and EMRC* will adopt a standardised taxonomy for roles, tasks, knowledge, and skills specific to the energy sector, ensuring alignment with national and international standards. They will also collaborate to define baseline cyber security controls for companies to implement and provide guidance to help companies implement governance frameworks, to enable consistent operational management across the sector.

Action 2: Identify and secure critical assets, develop tailored security risk management policies.

As a vital first step, **energy companies across the sector must identify and categorise their critical assets**, including IT and OT systems, based on their importance to the ongoing provision of essential services to the Kingdom. Companies should then assess the threats and vulnerabilities facing their critical assets to develop tailored security measures and risk management strategies to protect them. These measures will be integrated into a Business Continuity Plan (BCP) to ensure assets are protected and recoverable in the event of a disruption.

NCSC-JO will build and maintain a centralised Critical Asset Register, populated with data provided by the individual companies, which will provide a foundation for understanding and improving critical infrastructure resilience across the sector. This register will enable NCSC-JO and EMRC to prioritise support efforts and develop long-term plans for asset hardening, based on the criticality and risk profile of each asset. Once the Critical Asset Register is complete, NCSC-JO and EMRC will develop an intelligence-led approach to help companies to **identify, assess, and remediate vulnerabilities** in a structured and repeatable manner to drive continuous improvement.[9]

Companies will **independently adopt policies and procedures that comply with the Jordanian National Cyber Security Framework (JNCSF), and embed cyber security principles**, such as Security by Design, across both IT and OT systems. This includes developing and testing individual Disaster Recovery (DR) plans to address operational disruptions, including those caused by physical threats like flooding or other climate-related risks. DR plans should integrate the physical controls outlined in the Critical Infrastructure Cyber Security Controls (CICSC) to ensure resilience.[10]

[9] **Cybersecurity Best Practices Testing** (CBEST), developed by the UK's Bank of England with regulators and UK National Cyber Security Centre, provides a potential model for this form of testing. It uses real-time threat intelligence and penetration testing to assess vulnerabilities through simulated attacks and promotes collaboration between financial institutions, regulators, and intelligence agencies:

[10]

As part of these efforts, energy companies should also adopt a holistic approach to secure both **cyber and physical aspects of their critical communication infrastructure,** such as, Global System for Mobile Communications (GSM) networks, fiber optic cables, Long Range (LoRa) wireless communication systems, and IoT protocols. These channels are vital for operational resilience and must be protected using measures like encryption, advanced intrusion detection systems, and adherence to international security standards. Companies should integrate relevant controls, including those outlined in the Critical Infrastructure Cyber Security Controls (CICSC), into their broader risk management strategies to mitigate risks effectively and ensure synergy across the energy sector.

Finally, companies must establish robust **supply chain risk management policies** to strengthen the cyber security ecosystem supporting critical operations in Jordan's energy sector. It is the responsibility of individual companies to map and manage risks within their own IT/OT supply chains, linking these to the assets captured in the above outlined Critical Asset Register. This includes adopting the supply chain security (SR) controls outlined in the Critical Infrastructure Cyber Security Controls (CICSC) issued by NCSC-JO. These controls emphasize the importance of vendor risk management through cyber security standards, regular audits, and contractual obligations to enforce supply chain security.

Responsibilities:

- *Individual company* board management must task asset management teams to identify and categorise critical assets, share this information with NCSC-JO and EMRC, map and manage their own IT/OT supply chains, and ensure disaster recovery and risk management policies are developed and implemented.
- *NCSC-JO* will support and guide companies in identifying their critical assets, verify that critical assets are properly identified and secured, maintain the Critical Asset Register and provide a framework for monitoring and driving improvements.
- *EMRC* will support and guide companies in identifying their critical assets, ensure that the policies developed meet national security standards, oversee compliance, and support the adoption of effective supply chain controls.

Action 3: Implement regular risk assessments and compliance audits.

To establish a baseline understanding and management of cyber security risk, companies in the energy sector will need to implement a program of regular, cyclical risk assessments and compliance audits. These assessments will address systems and functions critical to business success, such as OT systems and energy distribution networks. Key activities involve real-time monitoring, penetration testing, analysing risks and managing them through controls that are subsequently audited.

The outcomes of these risk assessments should feed into a structured process where cyber security policies and procedures are reviewed and updated regularly. This ensures that security measures evolve in response to emerging threats and key vulnerabilities, thereby safeguarding critical infrastructure assets against current and future risks.

Responsibilities:

- *Individual companies* will be responsible for establishing risk assessment procedures to evaluate vulnerabilities and threats regularly. This includes deploying internal or external penetration testing teams to identify weaknesses in systems and assess technical and operational defences. Compliance departments, overseen by the CISO, will be responsible for enforcing policies, monitoring adherence to controls, and addressing gaps identified during assessments. Companies will also conduct periodic independent audits (with the help of internal and/or external auditors) to evaluate compliance with internal policies and sector standards. These audits should provide actionable recommendations for improving systems and processes.
- *NCSC-JO and EMRC* will oversee and provide initial guidance to help companies to ensure consistency across the sector, providing guidance for companies to align risk management and compliance practices with national benchmarks. They will also facilitate joint assessments to promote a unified approach to resilience.

Action 4: Secure board-level and senior management engagement.

To ensure strategic leadership in cyber security, each company across the energy sector must establish dedicated board-level ownership of cyber security. Boards must understand the risk that cyber incidents present to business strategy and ensure resilience to cyber attacks. As well as overseeing and championing these efforts at the highest level, the board should participate in quarterly cyber security briefings, regular risk assessments, and receive frequent updates on emerging threats.

The board should also have direct involvement in crisis management exercises. Distinct from operational IR drills outlined in Strategic Objective 3, these exercises ensure that roles and responsibilities are clearly defined and understood, while also testing and improving responses before a major incident occurs. This is particularly vital for managing communication of incidents to customers, regulators, and other stakeholders.[11]

By visibly prioritising cyber security, boards will shape and champion a security-first culture that permeates the entire company, enhancing internal and external credibility. Boards should also lead diversity and inclusion initiatives within cyber security teams, recognising that diverse perspectives and inclusive practices will enhance innovation and strengthen company defences.

Responsibilities:

- Board members and senior leadership within energy companies will ensure they receive quarterly briefings on cyber threats and business resilience to cyber incidents, set and oversee strategic cyber security objectives, allocate resources to talent development within cyber security, and model a commitment to cyber resilience.
- Training and HR teams will implement continuous board-level learning and awareness activities, support board-led diversity initiatives, and monitor company participation in cyber security activities.

[11] Guidance can be taken from https://www.ncsc.gov.uk/files/NCSC_Cyber-Security-Board-Toolkit.pdf.

2 Establish security operation capabilities

Vital to building individual and collective resilience, this objective will increase the energy sector's ability to detect, respond to, and recover from cyber security incidents. This will ensure the sector builds situational awareness, resilience and responsiveness to the fast pace of cyber threats.

Aims

The primary goal is to establish a robust incident detection, monitoring and response infrastructure that enables the energy sector to address cyber security threats efficiently and mitigate their impact. This requires companies to invest in the following:

- **Conducting security technology gap analyses** and securing funding for necessary cyber security tooling and upgrades.
- Establishing **individual SOCs** within each company[12] for real-time incident monitoring and response; individual basic **IR** capabilities, playbooks and exercises; and individual basic **CTI** capabilities, to ensure a sector-wide baseline of threat detection and response.
- Once established and operating effectively, connecting the individual SOCs to a **sectoral CERT** (En-CERT)**,** providing centralised coordination, intelligence sharing, and advanced response capabilities.[13]

High-Level Operational Plan

Action 1: Conduct individual technology gap analyses and secure funding for cyber upgrades.

To drive transformational improvement, this strategy requires each company in the energy sector to take a structured and proactive approach to enhancing cyber security technologies. Companies should begin with a detailed technology gap analysis across their IT and OT. This analysis should identify current cyber capabilities, security exposure, infrastructure gaps, and the risk posed to the continued provision of essential services without action. These assessments will help pinpoint existing vulnerabilities, evaluate existing tools and resources, and the identify priorities for addressing cyber threats effectively.

Based on these findings, companies will need to implement clear budgeting and prioritisation policies to ensure technologies deliver measurable value, and secure dedicated cyber security investment aligned with overall business strategy. Budget planning should prioritise immediate security needs, allowing for critical upgrades in exiting technologies to ensure they can support the energy sector's digital transformation. Planning should also cover adopting modern security tools and technology to enhance IT and OT security – including scalable technologies such as automated backup systems, cloud-based failover solutions, and data replication tools. These will enable swift recovery of essential systems and data following an incident. This aim reflects the National Cyber Security Strategy (2024-2028)'s emphasis on increasing financial commitment to cyber security.

Responsibilities:

- *Individual companies'* cyber security team, under the direction of a CISO or equivalent accountable officer, will conduct technology and risk audits across IT and OT to identify security gaps, infrastructure needs, and upgrade priorities. These will drive recommendations for immediate and scalable technology solutions to enhance cyber

[12] This could be in-house or delivered by a service provider.
[13] See Appendix A for the detailed stages of SOC and CERT set up.

resilience. Senior management will also oversee budget allocation and ensure investment in cyber improvement programmes that align with company goals and support the integration of scalable security technologies.

- *NCSC-JO and EMRC* will provide guidance, support and frameworks to companies to ensure consistent gap analyses and provide insights into threats and national cyber security priorities, enabling companies to make informed, aligned investment decisions independently.

Action 2: Establish individual Security Operations Centres (SOCs), Incident Response (IR) and Cyber Threat Intelligence (CTI) capabilities.

To transform cyber security across Jordan's energy sector, this strategy requires that each company within the sector establishes an **individual SOC** to centralise and co-ordinate the management of cyber security incidents and protect its digital assets. It should focus on immediate and specific security needs, employing real-time monitoring to detect and respond to potential threats quickly.

The SOC may be established in-house or provided by an authorised third party provider, but will need to include all technical operational security components - people, devices and tools - with the purpose of identifying any malicious activity. Third-party SOC services may offer a practical solution for entities unable to establish their own SOCs due to financial constraints. Leveraging such services can serve as a gateway for entities to eventually develop internal SOC capabilities.

From an operational basis, a phased approach to setting up a SOC will be essential to ensure success. Depending on current maturity levels, these stages will likely include: [14] [15]

[14] See Annex D for a more detailed implementation plan.
[15] Detailed guidance is provided by MITRE: '11 Strategies of a World-Class Cybersecurity Operations Center'. https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

- **Stage 1: SOC architecture design (2-4 months)** - Build the foundation for SOC operations in each company. Create an operating model, capability development plan, and decide on an individual resourcing model for SOC staffing. A key decision here will be between an in-house SOC or a managed service provider (MSP) contract, based on company needs. [1]
- **Stage 2**: **Core capability building (2-6 months)** - Develop essential SOC capabilities, including the centralisation of logs, implementing new firewalls, and Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) deployment to support real-time data collection and analysis.
- **Stage 3: SOC implementation (6-12 months)** – Implement SOC triaging and escalation processes and achieve full SOC functionality; establish various playbooks for day-to-day functions such as email analysis, alert triaging and host investigations.
- **Stage 4: Optimisation and capability expansion –** Depending on company complexity, criticality, and risk profile, enhance SOC functions with advanced capabilities such as Security Orchestration, Automation, and Response (SOAR), Machine Learning-enhance SIEM functions, red teaming, threat hunting, and behavioural analytics for improved automation and response.

Secondly**,** high-quality, consistent **IR capabilities** and regular security collaboration are vital to building resilience within and across the energy sector. Organisations in Jordan's energy sector must develop and implement individual, independent incident response policies and playbooks that align with national standards, with guidance from NCSC-JO or other regulatory bodies. Where required, companies will hire skilled personnel with the expertise needed to bridge capability gaps. Each company will also independently **exercise** its incident response capabilities, ensuring they can effectively respond to incidents without relying on sector-wide infrastructure. Exercises should test both technical and board-level responses, involve legal and communications specialists, as well as engagement regulators and suppliers. This will help to improve staff proficiency and co-ordination with peers and regulators, ensuring companies are better prepared to handle real attacks.

Finally, to enhance cyber threat detection and information-sharing across Jordan's energy sector, companies must develop **individual, foundational CTI capabilities**, to independently build their understanding of cyber threats, and manage and share threat intelligence.

Responsibilities:

- *Individual companies'* CISOs and cyber security team will direct the development and management of **SOCs**, including selecting, implementing, and optimising advanced threat

detection tools to be integrated into SOCs as they become fully operational.[16] *NCSC-JO* will provide a central coordination mechanism for initial log management and/or IR to support companies as they build their SOCs. It will provide guidance on SOC implementation, ensuring alignment with national standards, consistency and inter-operability – vital to effective sharing, mutual support, and building collective resilience across the energy sector.

- *Individual companies'* will develop individual **IR** plans and playbooks, hiring or upskilling personnel to bridge capability gaps as needed, ensuring sustainability in the long term. Company boards will conduct regular IR exercises, with CISOs ensuring company-wide participation to improve decision-making, communication, and legal response readiness. *NCSC-JO and EMRC* will provide blueprints, guidance, and to help support to individual companies shape robust individual IR strategies and effectively manage immediate threats.
- *Individual companies* will establish core **CTI** capabilities, led by CISOs, to enable independent threat understanding and management. *SOC and CTI teams* will handle data collection, analysis, and reporting to support incidents, continuity, and cyber security strategy, ensuring insights are shared promptly with sector peers. *NCSC-JO* will advise individual companies on establishing CTI capabilities, protocols and sharing agreements.

Action 3: Establish a sector-wide Computer Emergency Response Team (En-CERT).

Concurrently with the development of company capabilities and drawing on the successful approach implemented in Jordan's Finance Sector, the Government of Jordan will work with NCSC-JO, EMRC, and the Energy Sector to establish a **sector-wide Computer Emergency Response Team (En-CERT).** With support from NCSC-JO, EMRC will lead the establishment of En-CERT and head all En-CERT efforts, thus acting as the primary regulator and coordinator for cyber security within the energy sector.[17]

To facilitate the successful establishment and operation of En-CERT, EMRC will set up an internal **'Steering Group'**, responsible for coordinating all En-CERT-related efforts. This group will oversee the development of sector-wide IR standards, playbooks, and response mechanisms, ensuring alignment across all companies in the sector. The Steering Group will also define clear cross-sector collaboration processes, particularly for information sharing and joint response activities. This will include joint IR exercises, integrated into company-individual SOC activities, to enhance sector-wide preparedness.

While EMRC will manage En-CERT coordination and guidance, *individual companies will remain responsible for establishing their own SOCs* to meet their specific operational needs.

Once operational, En-CERT will:

- Define and formalise sector-wide **IR** policies, playbooks, and logging standards to ensure consistent and effective incident handling.
- Establish clear protocols and agreements for **CTI** sharing, collaboration, and secure information exchange among companies, EMRC, NCSC-JO, and JO-CERT. The protocols will leverage NCSC-JO's existing relations with firms to define structured sharing mechanisms that embed regular collaboration on cyber security across the energy sector.

[16] Detailed guidance is provided by MITRE: '11 Strategies of a World-Class Cybersecurity Operations Center'. https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf
[17] See detailed implementation plan in Annex E: En-CERT implementation stages.

- Receive and disseminating this threat intelligence on a **secure platform**, including Indicators of Compromise (IoCs) and threat actor profiles provided by NCSC-JO, ensuring timely awareness and coordinated action across the sector.
- Foster **partnerships with international organisations** such as CERT-EU and US-CISA to share expertise, benefit from global threat insights, and align with best practices in cross-sector coordination.
- Facilitate regular information exchange **meetings, training, and annual Table Top Exercises (TTX),** particularly with smaller companies, to build sector-wide capacity and foster resource sharing and coordination.

To aid these efforts, NCSC-JO, in partnership with the EMRC, will establish a real-time **Early Warning System (EWS)** to monitor public IP ranges and domain names of all energy sector companies in Jordan. The EWS will scan continuously for known IoCs, vulnerabilities, and abnormal activities that could signal cyber threats. When established, EWS alerts will be promptly shared through En-CERT, ensuring that relevant stakeholders receive actionable intelligence. This model may serve as a pilot project for broader national implementation.

Responsibilities:

- *EMRC* will lead efforts to establish and manage En-CERT, including setting up an internal Steering Group to coordinate activities, and acting as the primary regulator representing NCSC-JO in the energy sector. As part of this role, EMRC will oversee and monitor sector-wide training and exercises, and company progress on the various aspects of operational cyber capacity building, ensuring alignment with the strategic implementation roadmap.[18] EMRC will however not be responsible for tracking internal training efforts *within* individual companies as outlined in Strategic Objective 3.

- *En-CERT* will develop and implement overarching, sector-wide IR mechanisms, coordinating collaboration among all stakeholders. It will formalise sector-wide secure CTI sharing policies and communication protocols. It will leverage NCSC-JO intelligence to provide threat actor dossiers, facilitate regular sector-wide training and TTX, and organise at a minimum weekly calls and regular in-person meetings to share intelligence and strengthen sector collaboration.

- *NCSC-JO and EMRC* will jointly launch an **EWS** to monitor Jordan's energy sector for cyber threats, sharing alerts through En-CERT's secure platform.

[18] Outlined in Annex A.

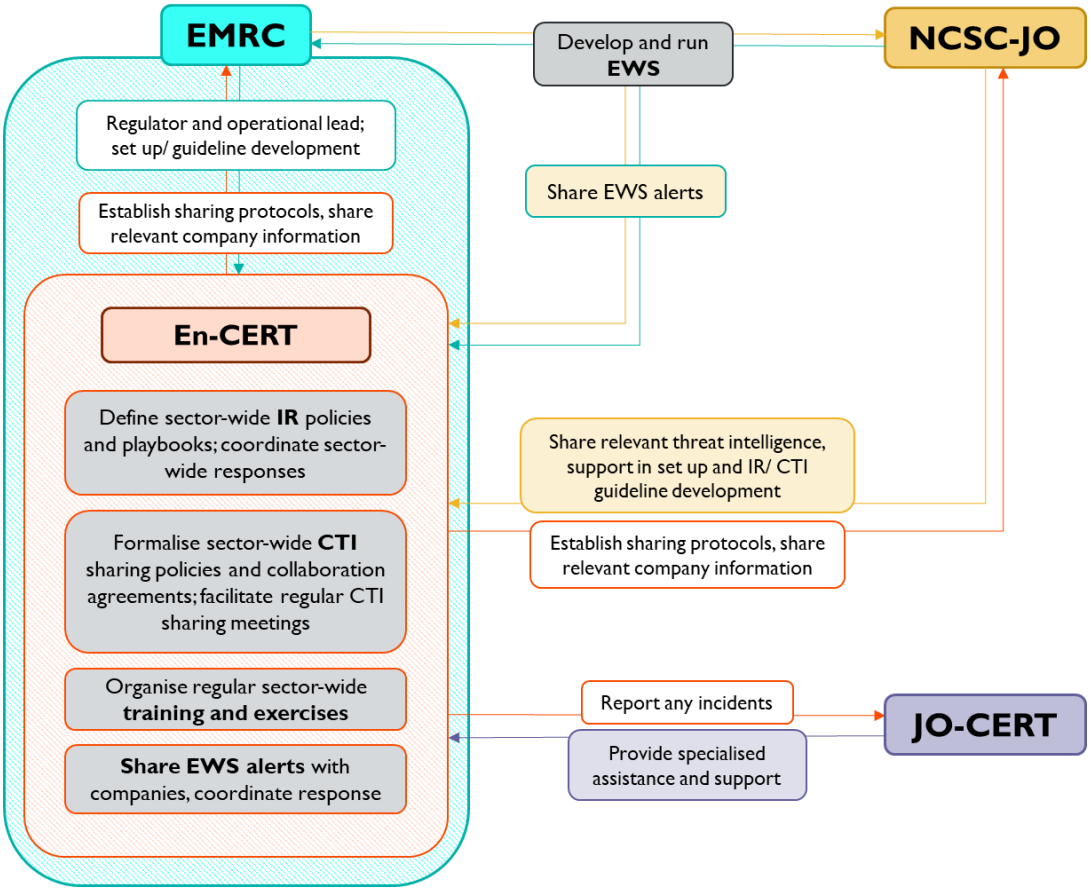

Figure 1: En-CERT division of responsibilities

Action 4: Launch an NCSC-JO embedding programme for IT and OT professionals.

To deepen the partnership with the energy sector, NCSC-JO will launch a **scheme to embed selected IT and OT cyber security professionals from energy operators within NCSC-JO** for 6 to 12 months in areas that provide mutual benefits in terms of skills and experience. This will strengthen direct, regular communication and allow for skills improvement and training. This will also solidify NCSC-JO's national cybersecurity efforts by in turn profiting from integrating current, actionable insights from operational challenges and trends, directly informing NCSC-JO's work and priorities.

Responsibilities:

- *NCSC-JO* will launch a program to embed energy sector cybersecurity professionals within NCSC-JO for 6–12 months, strengthening skills, communication, and sector-wide cybersecurity collaboration.

3 Develop cyber security skills and culture

This objective aims to cultivate a sector-wide culture of cyber security awareness and resilience, equipping employees across Jordan's energy sector with the skills to handle cyber incidents. It prioritises continuous training and awareness programmes designed to embed cyber security principles at every company level, from senior leadership to employees who are directly responsible for monitoring, detecting, and responding to security incidents within a company.

Aims

The primary goal is to increase cyber security awareness and skills across all levels within the energy sector. By fostering a pro-active security culture and delivering targeted, continuous training, this objective will:

- Ensure all employees understand and adopt cyber security best practices;
- Provide advanced training for key cyber security and IR personnel; and
- Build an environment of shared responsibility for cyber resilience, helping protect Jordan's energy infrastructure from evolving threats.

High-Level Operational Plan

Action 1: Implement regular training and practical exercises for the entire energy-sector workforce.

To effect change across the business, energy sector companies will implement a mandatory annual cyber security training programme for its employees at all levels, covering basic digital hygiene, phishing awareness, and incident reporting protocols. Given that phishing remains a key component of cyber attacks,[19] this will be supported by regular phishing simulations to test employees' vigilance and reduce social engineering risks. Additionally, tailored training modules will focus on OT-specific security needs to address skills gaps in OT IR.

To address the broader need for expertise and to upskill IT/OT employees, NCSC-JO will take the lead in integrating targeted initiatives to enhance workforce capabilities across the energy sector. Central to this effort will be the above outlined **NCSC-JO IT/OT Professionals Embedding Programme**, embedding experts from energy sector organisations to provide hands-on support and facilitate knowledge transfer. Complementing this, the development of **NCSC-JO's Cyber Academy** and ongoing work to train trainers within universities across Jordan will help ensure the provision and accessibility of high quality, practical cyber training to workers in critical infrastructure sectors.

Responsibilities:

- HR and security teams *within each company* will be responsible for designing and implementing annual training, as well as facilitating regular phishing simulations to test and drive continuous improvements in staff awareness and security behaviour and reporting the results to EMRC. Senior management will endorse the training programmes, model active participation, and ensure that all employees engage in these initiatives.

[19] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024 and Deloitte - 91% of all cyber attacks begin with a phishing email to an unexpected victim

- *NCSC-JO* will provide support and guidance in designing and implementing appropriate training, including through its Cyber Academy and its IT/OT Professionals Embedding Programme.
- *EMRC* will monitor the implementation of sector-wide training through En-CERT, and track strategic progress in line with the strategy implementation roadmap.[20]

Action 2: Build OT-specific skills through advanced training and strategic partnerships.

Given the vulnerabilities associated with OT, and its known targeting by various threat actors, a sustainable approach to workforce development is essential. Energy companies must provide advanced, role-specific training for IT and OT security professionals and IR teams, with a strong focus on OT threat detection and secure system operations. This should include fostering communities of practice across the sector to grow networks, share expertise, and sustain professional skills development. The aim is to ensure both immediate improvements in OT security and long-term resilience through capacity building.

Alongside this, NCSC-JO will play a key role by partnering with international organizations to offer certification programs and by prioritizing the integration of OT security into the NCSC-JO Academy curriculum to build national capacity to train and develop OT security skills.

Responsibilities:

- *Security and IT/OT teams* within energy companies will be responsible for identifying key personnel for advanced training (with a specific focus on OT-specific skills), appropriate training providers, enrolling them in certification courses, and monitor skills development to ensure practical application. Teams should actively build and engage in communities of practice to share expertise and promote sector-wide collaboration. *Senior management* within energy companies must allocate sufficient budget for advanced training, prioritizing OT and IR capabilities.
- *NCSC-JO* will partner with international organizations to facilitate certification programs that target OT cyber security. It will also integrate OT-specific training into the NCSC-JO Academy curriculum, and play a supportive role in fostering communities of practice to connect professionals, encourage expertise sharing, and strengthen the sector's collective defence.

[20] See Annex A.

Outlook and Conclusion

The Kingdom of Jordan is committed to building a robust cyber security foundation for its energy sector, recognising that reliable energy is essential for national resilience, security, and economic prosperity. This strategy for 2025–2028 outlines a bold and comprehensive approach to transform the cyber resilience of Jordan's energy infrastructure, ensuring its secure digital transformation and ability to withstand escalating cyber threats that could disrupt vital services for households, businesses, and essential industries. By focusing on developing critical cybersecurity capabilities — strengthening governance and policy, establishing SOCs, IR and CTI and a sectoral CERT, and developing cyber security skills — the strategy lays strong foundations for a secure, resilient energy sector.

Next steps and implementation

The successful implementation of this strategy relies on a coordinated, collaborative approach across all stakeholders. NCSC-JO and EMRC will take the lead in raising awareness, understanding, and support for the strategy with energy companies and providing clarity and ensuring alignment with strategic objectives. NCSC-JO and EMRC will also play a crucial role in bringing stakeholders together, fostering a collaborative environment where organisations across the sector can discuss and overcome challenges and share lessons learned to enable the effective roll-out of the strategy.

Regular progress reviews will be conducted throughout the lifetime of the strategy to assess progress and identify areas where adjustments may be needed. These reviews will provide high-level insights into the implementation process, ensuring the primary focus remains on achieving the outlined objectives.

Outlook

This strategy is not an endpoint, but a starting position that lays the groundwork for continuous improvement in the Kingdom's cyber resilience. It will be tracked and updated as Jordan moves along its journey towards a cyber secure and resilient future and will serve as a model for upcoming cyber security strategies across other critical sectors

Annex A: Detailed Strategy Implementation Roadmap

	Strategic Objective 1: Strengthen governance and policy			
	Action 1: Establish clear roles, responsibilities, and governance across the energy sector.	**Action 2:** Identify and secure critical assets, develop tailored security risk management policies.	**Action 3:** Implement regular risk assessments and compliance audits.	**Action 4:** Secure board-level and senior management engagement.
YEAR 1	• All individual companies in the energy sector have completed an initial review of their cyber security roles, responsibilities, and governance structures, identifying gaps and aligning with NCSC-JO standards. • NCSC-JO and EMRC finalise cyber security controls, defining minimum requirements for governance, IR, and technical safeguards.	• All Individual companies identify, categorise, and assess critical IT and OT assets, develop tailored asset protection plans, and establish security risk management policies integrated in Business Continuity Plans (BCP). • 100% of individual companies have identified their critical assets and applied tailored security measures and BCPs.	• All companies have established a regular policy review cycle (at least annually) to ensure policies remain aligned with current threats and best practices, and provide evidence to regulatory bodies. • Regular compliance audits are launched, with NCSC-JO and regulatory bodies ensuring consistency and sector-wide application of standards.	• Ensure 100% board attendance in quarterly cyber security briefings and active involvement in strategic cyber security planning.
YEAR 2	• Individual companies begin implementing standardised taxonomies, governance structures, and sector-specific controls developed by NCSC-JO and EMRC. • EMRC audits ensure Individual companies are maintaining and updating their governance structures to meet evolving cyber security requirements.	• Individual companies implement security principles in all new IT/OT systems and finalise tailored security risk management policies addressing security by design, disaster recovery (DR), and supply chain risk management. Policies will ensure IT/OT integration is consistent and meet NCSC-JO requirements. • NCSC-JO and EMRC have establish asset register, introduce a framework to identify and test vulnerabilities, enabling individual companies to drive continuous improvements in asset protection.	• 80% of Individual companies have adopted automated tools for continuous compliance monitoring, enabling rapid detection of policy breaches and real-time alignment with compliance standards.	• Launch of board engagement programmes with quarterly briefings and continuous updates through 2028. • Annual reports highlight board support for female and diverse representation in cyber security roles and significant resource allocation to resilience initiatives.

	Strategic Objective 1: Strengthen governance and policy			
	Action 1: Establish clear roles, responsibilities, and governance across the energy sector.	**Action 2:** Identify and secure critical assets, develop tailored security risk management policies.	**Action 3:** Implement regular risk assessments and compliance audits.	**Action 4:** Secure board-level and senior management engagement.
YEAR 3	• 100% of Individual companies achieve full implementation of controls, with critical cyber security roles filled by skilled individuals. • Independent evaluations by NCSC-JO confirm compliance and measurable improvements in cyber resilience across the energy sector.	• Individual companies conduct annual reviews of critical assets, ensuring ongoing security and risk management. • Continuous updates to BCP, DR, and supply chain risk management policies align with evolving risks and threats.	• A 100% compliance rate is achieved across all Individual companies, with annual audits verifying continued adherence to policies and standards.	• Continuation of above detailed initiatives.
YEAR 4	• Continuation of above detailed initiatives.	• Continuation of above detailed initiatives.	• Annual reviews ensure ongoing security and risk management of all identified critical assets, with continuous improvements to disaster recovery (DR) and supply chain risk management policies.	• Demonstrate measurable progress in fostering an inclusive workforce, reflected in improved employee survey results on cyber security confidence and awareness, displaying a robust security culture driven by board leadership.

	Strategic Objective 2: Establish security operation capabilities			
	Action 1: Conduct individual technology gap analyses and secure funding for cyber upgrades.	**Action 2:** Establish individual SOCs, IR and CTI capabilities.	**Action 3:** Establish a sector-wide Computer Emergency Response Team (En-CERT).	**Action 4:** Launch an NCSC-JO embedding programme for IT and OT professionals.
YEAR 1	• 100% of individual companies have completed a technology audit, gap analysis, and identified priority areas for cyber security investment.	• By Mid-Year 1 (July 2025): Individual companies complete Stage 1 of SOC establishment. • Individual companies have core IR capabilities established, ensuring consistent handling of incidents and the	• Begin establishment of foundational En-CERT architecture. • NCSC-JO begins development of the Early Warning System (EWS).	• NCSC-JO defines the programme structure, including objectives, selection criteria, and roles for IT and OT professionals. • NCSC-JO identify first candidates for the embedding programme.

		development of foundational IR playbooks. • Individual companies start developing foundational CTI capabilities to enable independent threat management. • By End of Year 1 (December 2025): Individual companies complete Stage 2 of SOC establishment.		
YEAR 2	• Individual companies have allocated initial funding by December 2025 and prepare multi-year programme plans and funding agreements.	• Individual companies have completed Stage 3 of SOC establishment, and deployed key tools such as Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) systems. • Individual companies start conducting at least annual IR exercises, incorporating lessons learned to improve playbooks, response times, and staff preparedness. • 80% of individual companies have set up foundational CTI capabilities and actively participate in intelligence exchanges.	• En-CERT architecture is operational, with shared IR resources available through a secure platform. • En-CERT launches a CTI sharing platform, enabling all organisations to access actor dossiers and participate in regular information exchanges. • En-CERT-led sector-wide IR exercises commence annually across all organisations to ensure alignment, readiness, and continuous improvement. • NCSC-JO's EWS is operational, providing alerts to organisations that are distributed via En-CERT.	• NCSC-JO launched the embedding programme, onboarding the first cohort of IT and OT professionals for 6–12 month rotations. • NCSC-JO evaluates the progress of the first cohort and gather feedback from participants and energy operators to refine the programme.
YEAR 3	• At least 85% of individual companies have allocated funding and invest it based on their identified cyber security priorities.	• Individual companies conduct annual maturity assessments of CTI capabilities and report results to NCSC-JO and EMRC. • At least 75% of incidents are detected and responded to within 24 hours, as measured by SOC performance reports.	• En-CERT and NCSC monitor sector-wide improvements in situational awareness, threat detection, and intelligence sharing, refining the EWS and CERT capabilities as needed.	• NCSC-JO regularly rotates new cohorts into the programme to sustain collaboration and skills development.

YEAR 4	• Continuation of above detailed initiatives.	• Individual companies commence Stage 4 of SOC establishment.	• Continuation of above detailed initiatives.	• Continuation of above detailed initiatives.

	Strategic Objective 3: Develop cyber security skills and culture	
	Action 1: Implement regular training and practical exercises for the entire energy-sector workforce.	**Action 2:** Build OT-specific skills through advanced training and strategic partnerships.
YEAR 1	• Individual companies launch initial training programmes and conduct the first phishing simulations. • 100% of employees complete the initial training, with annual refresher completion rates of at least 90%.	• Individual companies launch advanced training for designated IR and OT team members, with annual updates and skills assessments through 2028. • 100% of designated IR and OT team members complete the initial advanced training.
YEAR 2	• Individual companies achieve a 65% reduction in successful phishing attempts compared to the 2025 baseline.	• Individual companies achieve a 30% reduction in OT IR times, demonstrating improved team capabilities.
YEAR 3	• Continuation of above detailed initiatives.	• Employees report a 50% improvement in confidence in IR capabilities.
YEAR 4	• Continuation of above detailed initiatives.	• Continuation of above detailed initiatives.

Annex B: Alignment with national cyber regulation

This strategy will support NCSC-JO to engage with and build cyber resilience in the nation's energy sector. To sustainably achieve this aim, it is closely aligned with overarching Jordanian regulation, namely the **National Cyber Security Strategy (2024-2028)**, and Jordan's **National Cyber Security Framework 2024** (JNCSF – see figure below).

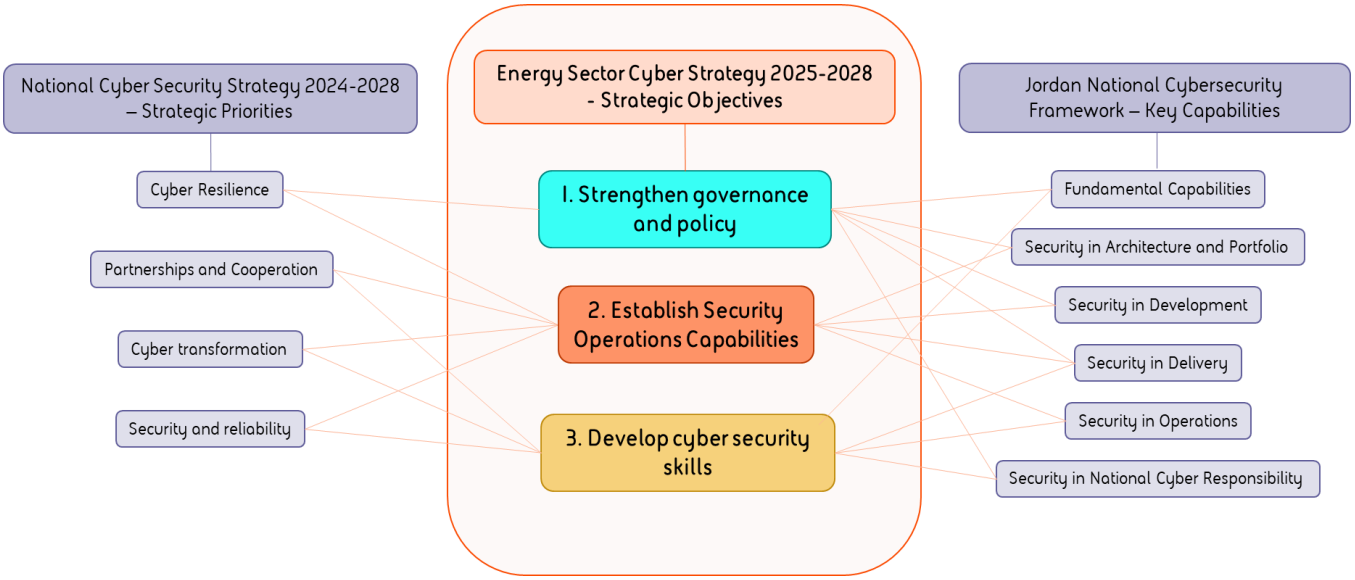

Figure 2: Alignment between the proposed Strategic Objective, the National Cyber Security Strategy (2024-2028), and the JNCSF

Annex C - The Challenge: Detailed analysis

The necessity for this strategy is driven by a range of serious and urgent challenges and opportunities, which collectively demand improvements to the cyber security of Jordan's energy sector. These include:[21]

1 Political

Since the creation of JO-CERT and NCSC-JO, Jordan's government has made significant strides in prioritising cyber security for critical infrastructure, including in the energy sector. Jordan's National Cyber Security Framework 2024, along with the National Cyber Security Strategy (2024-2028), provide a solid framework for ensuring a high standard of cyber security. In addition, government-backed initiatives encouraging collaboration with both private stakeholders and international partners in the Gulf and beyond strengthen Jordan's ability to defend itself against advanced cyber threats. Jordan's progress in the Global Cybersecurity Index (GCI) reflects these efforts.

Despite these developments, policy gaps remain in sector-specific regulations for energy, leading to inconsistent practices across companies and thus increasing the vulnerability of the Kingdom's energy infrastructure to cyber attacks. Diverse stakeholder priorities may complicate the creation of a unified cyber security approach. While government bodies and regulators, such as NCSC-JO and EMRC, are focused on national security and regulatory compliance, private energy operators may prioritise operational efficiency and cost considerations. Aligning these priorities – forging mature partnerships - is essential to building a robust cyber strategy. Jordan's proximity to regional conflicts increases the likelihood of cyber actors targeting Jordan's critical infrastructure, adding further urgency to need to enhance defensive measures and cross-border coordination.

2 Economic

Jordan's energy sector, particularly in renewable energy, attracts substantial foreign investment and offers an opportunity to fund cyber security investments. The country's stability, relative to its regional neighbours, creates a conducive environment for long-term investments in safeguarding critical assets. Growing national investment in projects such as solar and wind farms, combined with rising awareness of cyber security within major energy companies, align with the Government's ambition to stimulate the Jordanian cyber security industry and market.

However, budget constraints, particularly in small and medium-sized enterprises (SMEs), limit the sector's ability to make progress at the pace needed. The sector's reliance on foreign aid and loans exacerbates these financial challenges, potentially delaying critical upgrades. Additionally, the current regulatory environment lacks strong enforcement mechanisms or penalties[22] to incentivise compliance and allocate larger budgets to cyber security as a regulatory necessity. Finally, a lack of board-level cyber security awareness and inadequate budget allocation weakens the overall resilience of the sector, leaving it vulnerable to supply chain risks and unprotected critical assets.

3 Social

Public and governmental awareness of cyber security is growing, providing a strong foundation for enhancing security measures. Government efforts to secure the energy infrastructure are driven by the need to meet the needs of Jordan's people, who expect and deserve uninterrupted services.

[21] Please find the complete, extended analysis in Annex C: The Challenge.
[22] Such as those enforced under the European General Data Protection Regulation (GDPR).

However, the sector faces a shortage of skilled cyber security professionals, particularly in specialised areas such as OT security, which remains a critical concern. Limited awareness of cyber security risks among energy sector employees further exacerbates this issue, making workforce development a top priority. While universities are expanding cyber security programmes, practical experience within these courses remains insufficient. Though government initiatives promote women's participation in Science, Technology, Engineering, and Mathematics (STEM) fields, their representation in cyber security roles after graduation remains low. Jordan's important role in caring for refugees heightens the need for strong cyber security defences to ensure continuous energy services. Addressing these challenges through targeted capacity-building initiatives is essential to enhancing the resilience of Jordan's energy sector, fostering public trust in digital services, and creating employment opportunities, particularly for under-represented groups.

4 Technological

Jordan is actively working to transform its energy sector to provide greater security and reliability through the adoption of advanced technologies such as smart grids and digital energy management systems. However, the successful deployment of these innovations requires careful integration with security and data protection considerations from the outset. Without proper design, there is a risk that these technologies will be deployed into existing, insecure networks that rely on outdated legacy systems, undermining their effectiveness and exposing critical systems to cyber threats. Legacy systems often lack resilience and advanced capabilities, such as endpoint detection, AI-driven threat detection, and quantum-resistant encryption, requiring focused upgrades to address inherent vulnerabilities.

The increasing convergence of IT and OT environments further complicates the security landscape, introducing new attack vectors in critical systems that are often inadequately protected. Many organisations in the sector are not fully equipped to manage this convergence, leaving gaps in protection and creating additional challenges for maintaining cyber resilience.

Emerging technologies and associated threats, such as AI-enabled attacks that may exploit automation and supply chain vulnerabilities, pose significant risks. Additionally, quantum computing may undermine traditional encryption methods, necessitating proactive investment in quantum-resistant technologies.

While some companies have implemented basic defences and developed or are in the process of developing SOCs, many lack comprehensive IR frameworks or advanced threat detection capabilities. This uneven maturity across the sector leaves it ill-prepared to manage and recover from to sophisticated and emerging threats, and serious cyber incidents.

5 Environmental

Jordan's commitment to expanding renewable energy sources presents an opportunity to embed cyber security measures into new, greener infrastructure from the outset. Governmental backing also drives investment in upgraded services, fostering innovation and greater awareness of cyber security needs. However, climate change-related risks, such as extreme heat, flooding or natural disasters, threaten infrastructure stability and operational continuity. While disaster recovery (DR) and business continuity plans (BCP) are crucial for mitigating these risks, inconsistent investment and implementation across the sector leave critical systems vulnerable. These risks underscore the need to integrate physical controls, such as flood protection measures, into infrastructure planning and cross-reference them with cybersecurity measures outlined in the Critical Infrastructure Cyber Security Controls (CICSC).

6 Legal

Building on solid foundations, Jordan is continuing to expand its regulatory framework for cyber security, such as through the launch of the Cybercrime Law 17/2023 in 2023, and Jordan's National Cyber Security Risk Framework in 2024 – which will raise standards across Jordan's government and critical infrastructure. A regulatory drive to align with international legislation and standards, such as the European Union's General Data Protection Regulation (GDPR) and the ISO frameworks will further enhance security while promoting cross-border co-operation and improving Jordan's global standing in cyber security. However, currently, Jordan has relatively few cyber specific laws and regulations governing its Critical National Infrastructure, and the legal framework for the energy sector is still evolving. Key gaps remain, such as a lack of dedicated protections for critical assets and insufficient resources for conducting regular audits. Helping companies to adopt effective standards while strengthening regular compliance checks are essential to bolster the resilience of Jordan's energy infrastructure.

Annex D – SOC implementation stages

Stage 1: Policy and governance, design security architecture

This first step involves designing the security architecture for individual SOCs within each company to enable real-time incident monitoring and response. This includes conducting a capability gap analysis to assess current capabilities against operational requirements, and creating a capability development plan including an individual resourcing model for required SOC staffing. Organisations can either build their own SOC or establish a managed service provider (MSP) contract, depending on their needs; if using an MSP, a small, dedicated IR team should be established in-house for oversight. To plan, implement, and manage their SOCs effectively, companies should select and align with tested frameworks based on international best practices.[23] This stage should take 2–6 months.

Stage 2: Build initial capabilities – collect logs, EDR

With the above foundation in place, companies should establish log management, and building the SOC's core capabilities. Organisations should focus on collecting and centralising logs while upgrading their technology stack where possible for scalability and enhanced data analysis. This includes deploying Endpoint Detection and Response (EDR) systems, install and configure new firewalls, and establishing a central logging repository to support real-time monitoring. This phase should take approximately 2–4 months.

Stage 3: SOC implementation

As capabilities take shape, the SOC is implemented to provide full operational capabilities. Newly implemented tools and technologies should be securely configured according to international best practices, such as correctly implementing preventive measures to mitigate initial access risk, and configuring Active Directory.[24] A shared platform for CTI and IR reporting should be implemented to facilitate streamlined communication and allow for protective monitoring across the sector. This stage typically takes 6–12 months to complete.

Stage 4: Optimisation and growth

Once core operations are stable, the final stage involves optimising and expanding SOC functions. This may include adding advanced capabilities like audit functions, red teaming, threat hunting, analytics, and Security Orchestration, Automation, and Response (SOAR) tools to automate processes. The aim is to expand SOC coverage, enhance threat detection and response, and continuously improve operational efficiency through these advanced tools and practices.

---

[23] Options include for example the SOC Capability Maturity Model (SOC CMM), which helps assessing and developing SOC capabilities, and/or the NIST Cybersecurity Framework (CSF) 2.0, which offers a comprehensive approach to managing cybersecurity risks and develop comprehensive security protocols.

[24] Captured for example in these resources: https://www.cyber.gov.au/sites/default/files/2024-09/PROTECT-Detecting-and-Mitigating-Active-Directory-Compromises.pdf and https://www.huntress.com/blog/addressing-initial-access.

Annex E – En-CERT implementation stages

Stage 1: Foundational structures

In parallel with the SOC development, foundational structures for a sectoral Computer Emergency Response Team (En-CERT) will be established that provides and coordinates IR and CTI capabilities across the sector. This begins with defining policies IR to ensure consistent logging and incident handling across companies, along with developing and scheduling regular IR exercise plans, and establishing protocols for streamlined CTI sharing with the CERT. This stage should take 2–6 months.

Stage 2: Build initial En-CERT capabilities

With the foundation set, the next stage focuses on building initial En-CERT capabilities. Companies' logs are fed into the En-CERT for aggregated analysis, while tools are deployed to support IR and CTI analysis at a sectoral level. This stage lays the groundwork for centralised coordination and usually takes 2–4 months.

Stage 3: En-CERT implementation

The implementation of the En-CERT brings together coordinated capabilities for IR and CTI sharing across the sector. Reporting channels for protective monitoring should be established, and a shared platform for IR reporting and CTI communication should be impemented to facilitate collaboration. This phase should take 6–12 months to complete.

Stage 4: Optimisation and growth

Once operational, the En-CERT should focus on optimisation and growth. Advanced functions such as analytics, proactive threat hunting, and red teaming should be introduced, and processes will be optimised through automation tools. Continuous improvement should be emphasised through regular reviews and updates to align with evolving sector needs.

المركـز الوطنـي للأمـن السيبرانـي
National Cyber Security Center

National Cyber Security Center
Amman - 7th Circle +(962) 6 900 500 +(962) 65 300 265 Info@ncsc.jo