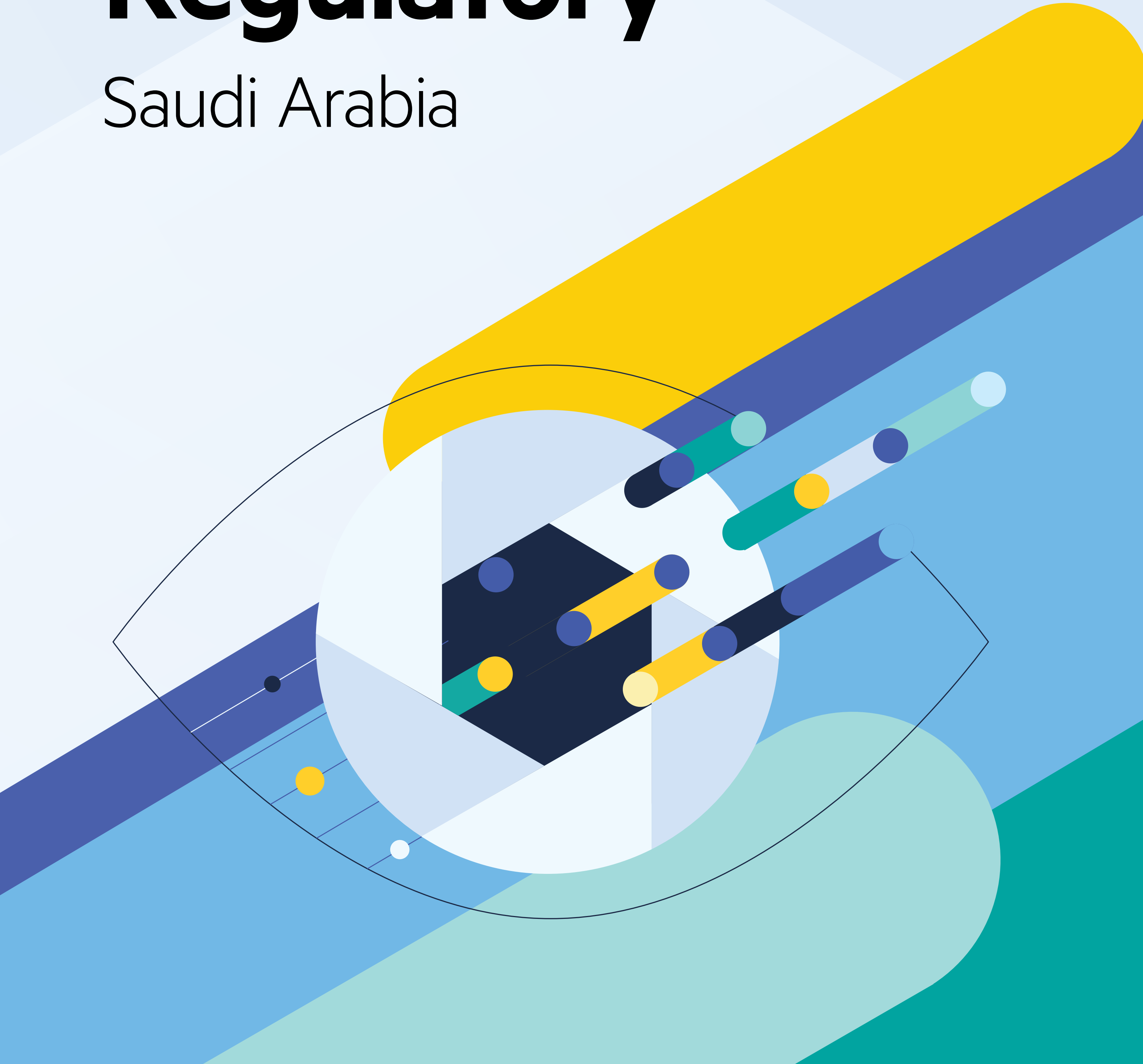
Progress® Flowmon®

Compliance Regulatory

Saudi Arabia



What is the Kingdom of Saudi Arabia's Cyber Security regulation?

The National Cybersecurity Authority (NCA) established as part of the Kingdom of Saudi Arabia's 2030 Vision is the central authority responsible for overseeing cybersecurity in Saudi Arabia. It plays a crucial role in formulating policies, guidelines, and regulations to protect critical infrastructure and mitigate cyber threats. Its mandate was approved as per the **Royal Decree number 6801, dated 11/2/1439H** making it the national and specialized reference for matters related to cybersecurity in the Kingdom.

NCA developed 3 main cybersecurity controls within years 2018 – 2020:

- ECC (1:2018) **Essential Cybersecurity Controls**, a set of guidelines and requirements issued by the NCA. These controls provide a framework for organizations to enhance their cybersecurity posture and protect critical information infrastructure. They cover various aspects of cybersecurity, including governance, risk management, access controls, incident response, and security monitoring.

- CSCC (1:2019) **Critical Systems Cybersecurity Controls**, as an extension of ECC specifically tailored to safeguard critical systems and infrastructure. These controls aim to protect critical infrastructure sectors such as energy, water, transportation, healthcare, finance, and telecommunications against cyber threats.

- CCC (1:2020) **Cloud Cybersecurity Controls,** as an extension of ECC contains specific guidelines and controls for ensuring the secure adoption and usage of cloud services in Saudi Arabia. These controls focus on protecting sensitive data and mitigating the risks associated with cloud computing.

Am I Regulated Entity?

Subject Regulated Entities (SREs) are the entities that are a subjects to the Cybersecurity Regulation in SA and contains:

ECC (1:2018):

- **Critical Infrastructure Operators**, entities that operate and maintain critical infrastructure sectors such as energy, water, transportation, healthcare, finance, and telecommunications.

- **Government Agencies**, entities at the federal and local levels are also considered subject regulated entities. This includes ministries, agencies, and other government organizations that handle sensitive information or provide critical services.

- **Digital Service Providers**, entities that provide digital services These include cloud service providers, managed security service providers, domain registrars, and other entities involved in the provision of digital services.

CSCC (1:2019):

- **Industrial Control Systems (ICS) Operators** that own or operate industrial control systems. These systems include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other operational technology (OT) systems.

CCC (1:2020):

- **Cloud Service Providers (CSPs)** that offer services in Saudi Arabia. These are the entities that provide cloud infrastructure, platforms, or software services to customers.

- **Cloud Service Tenants (CSTs)**, any government organization in the Kingdom of Saudi Arabia inside or outside the Kingdom (including ministries, authorities, establishments and others) and its companies and entities, as well as private sector organizations owning, operating or hosting Critical National Infrastructures (CNIs) that currently use or planning to use any cloud service.

As an SRE means that you are subject to specific cybersecurity requirements designed to protect your infrastructure from cyber threats. The regulation requires you to implement appropriate **security measures** to prevent and report significant cybersecurity incidents that occur to the NCA.

Cybersecurity measures – Although the measures within the framework of ECC and their extension CSCC and CCC are similar, they differ in structure and designation, and in some cases, they also differ in individual measures like:

- **Networks Security Management**
- **Information System and Information Processing Facilities Protection**
- **Cryptography**
- **Cybersecurity Event Logs and Monitoring Management**
- **Cybersecurity Incident and Threat Management**
- **and more...**

How can Flowmon help you be ECC, CSCC and CCC compliant?

Flowmon is a comprehensive i**ntelligent network security monitoring solution** that provides **real-time visibility** into **network traffic** and helps organizations detect cyber threats and respond to cyber incidents. Flowmon can help you achieve compliance with the above Cybersecurity regulations trough targeted approaches like **Threat Detection** and **Threat Hunting**, **Incident Response** and **Digital Forensics, Hybrid Cloud Monitoring** and **Encrypted Traffic Analysis**, **Root Cause Analysis** and **Performance Monitoring** in single pane of glass.

Machine Learning

Adaptive Baselining

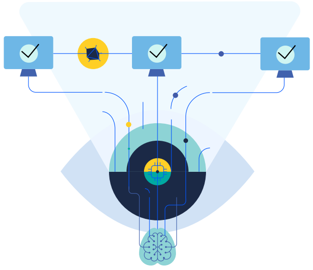
Heuristics

Behaviour Patterns

Reputational Data

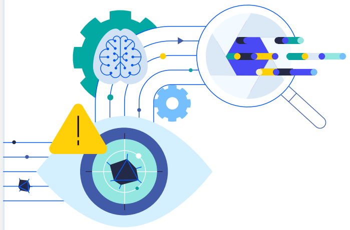
Signatures

Inteligence



200+ **Individual Algorithms**

40+ **Detection Methods**



Long Term Data Collection & Interpretation

Threat & Anomaly Alerts & Event Evidence

Here's how Flowmon can help you achieve **(2) Cybersecurity Defense Domain** and **(3) Cybersecurity Resilience** compliance:

1. Subdomain **Networks Security Management** ensures the protection of organization's network from cyber risks. Flowmon provides continuous monitoring and compliance audit if all controls are implemented in proper way, detection of behavioral anomalies, attacks, suspicious and malicious traffic communication and security policies violation within Controls **2-5-3 (ECC), 2-4-1 (CSCC)** and **2-4-P-1 (CCC)**.

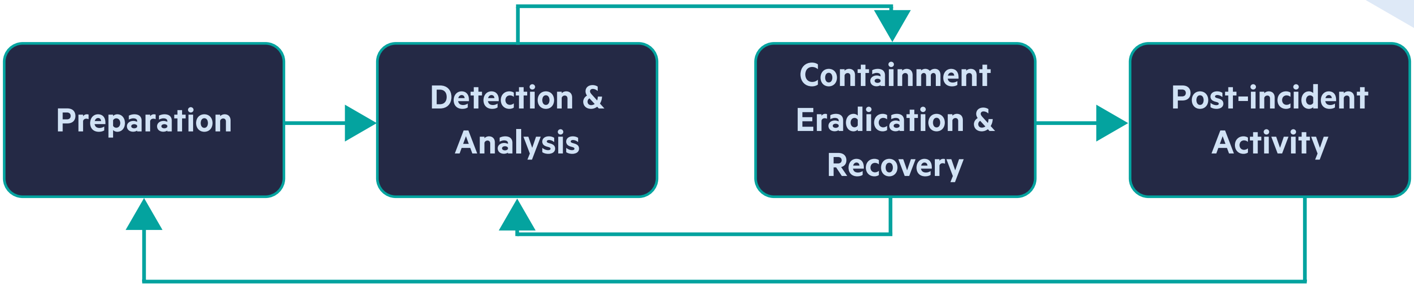
2. Subdomain **Information System and Information Processing Facilities Protection** within **CSCC** and Subcontrols **2-3-1-4** requires allocating specific workstations in an isolated network (Management Network), that is isolated from other networks or services

(e.g., email service or internet), **2-3-1-5** requires encrypting the network traffic of non-console administrative access for all technical components of critical systems and **2-3-1-8** requires protecting systems' logs and critical files from unauthorized access, tampering, illegitimate modification and/or deletion. Flowmon continuously monitor critical assets and services, their network communications to ensure network segmentation is deployed properly. Moreover, trough Encrypted Traffic Analysis (ETA) capabilities monitor ciphers suites, certificates or types of key algorithms. If any lateral movement of attacker inside critical infrastructure is happening, Flowmon detects unexpected behavior in real time, analyzes in autonomous way and responds immediately.

3. Subdomain **Cryptography** ensures the proper and efficient use of cryptography to protect information assets as per organizational policies and procedures regarding these regulations. Flowmon is able to monitor, check and audit if requested cryptography is used per organization, network segment, critical assets or services within Control **2-8-2 (ECC)** and Subcontrols **2-7-1-1 (CSCC)**, **2-7-P-1-1** and **2-7-T-1-1 (CCC)**.

4. Subdomain **Cybersecurity Event Logs and Monitoring Management** ensures timely collection, analysis and monitoring of cybersecurity events for early detection of potential cyber-attacks in order to prevent or minimize the negative impacts. As Flowmon is using mainly for network monitoring of cybersecurity events (attacks, misconfigurations, user or network suspicious behavior, vulnerabilities, outages etc.) which forward within aggregated form directly to SIEM for advanced correlation. That helps to comply with Subcontrols **2-12-3-3, 2-12-3-4 (ECC), 2-11-1-3, 2-11-1-4 (CSCC)** and **2-11-P-1-5 (CCC)**. Moreover, Flowmon provides the most powerful IPFIX Collectors for long term data retention period which require Subcontrol **2-12—3-5 for 12 months (ECC)** and Control **2-11-2 for 18 months (CSCC)**.

5. Subdomain **Cybersecurity Incident and Threat Management** ensures timely identification, detection, effective management and handling of cybersecurity incidents and threats to prevent or minimize negative impacts. This is all about incident handling and response procedures where Flowmon plays crucial role in many phases related standards like NIST. It helps to be compliant with Subcontrols **2-13-3-3, 2-13-3-4, 2-13-3-5 (ECC)** and **2-12-P-1-4, 2-12-P-1-5, 2-12-P-1-6 (CCC)**. Developing incident response plans is part of Subcontrol **3-1-3-2 (ECC)**.



Although there are no penalties set out in the ECC all SREs must report all significant incidents to NCA (as a cybersecurity competent authority within Kingdom of Saudi Arabia) responsible also for education, training, and raising awareness about cybersecurity through establishing affiliated centers.

Learn More About Progress Flowmon and Try Demo: www.flowmon.com

Progress