The National Cybersecurity Authority (NCA) within the Kingdom of Saudi Arabia (KSA) produces, and will periodically update, the Essential Cybersecurity Controls (ECC). The objective of the NCA is to ensure organisations maintain and support the cybersecurity of the Kingdom to protect its interests, national security, critical infrastructure, high priority sectors, and government services.

**ECC in-depth**

The main objective of the controls within the ECC is to set the minimum cybersecurity requirements for information and technology assets in organisations within the Kingdom. The requirements are based on industry leading practices which intend to help organisations minimise cybersecurity risks that originate from internal and external threats.

The published ECC cover the following key objectives:

- Confidentiality
- Integrity
- Availability

The controls cover the following cybersecurity pillars:

- Strategy
- People
- Processes
- Technology

All organisations within the Kingdom are highly encouraged to implement all controls associated with the ECC framework to improve and enhance their cybersecurity. All national organisations (including private sector organisations owning, operating, or hosting Critical National Infrastructures (CNI’s), must implement all necessary measures to ensure continuous compliance with the ECC as per item 3 of article 10 of NCA’s mandate and as per the Royal Decree number 57231, dated 10/11/1439H (June 25th, 2018). More detailed information on the ECC may be found [here](#).

**Benefits**

- Provide the flexibility to realise value at any point along the compliance maturity scale
- Meet ECC guidelines by collecting, managing, and analysing log data
- Enable your organisation to satisfy certain control families outlined by the ECC:
  - Identity and Access Management
  - Data and Information Protection
  - Incident and Threat Management
  - Vulnerability Management
- Generate regular reports that show exactly what has been achieved and identify any further steps that might be required
- Decrease cost of meeting ECC recommendations through prebuilt content and functionality.
The LogRhythm KSA-ECC module

The LogRhythm NextGen SIEM Platform enables your organisation to meet many ECC guidelines by collecting, managing, and analysing log data. LogRhythm AI Engine (AIE) rules, alarms, reports, investigations, and general SIEM functionality also help your organisation satisfy certain controls outlined by the ECC.

LogRhythm understands that organisations may be at different points of compliance maturity, so the KSA-ECC module gives organisations the flexibility to realise value at any point along that maturity scale. The KSA-ECC module is focused on the control requirements traditionally used for best practice purposes. LogRhythm supports some ECC recommendations and decreases the cost to meet others through prebuilt content and functionality. Using advanced LogRhythm functionality such as NetMon, TrueIdentity™ SysMon, threat research content, and case management may enhance prebuilt content to better support an organisation’s compliance efforts.

The KSA-ECC Module was built using LogRhythm’s Consolidated Compliance Framework (CCF) content, which cross-maps numerous globally accepted frameworks to demonstrate compliance across multiple jurisdictions. As LogRhythm’s technology stack grows and expands, we continuously enhance our CCF methodology to provide the highest-quality product to our customers.

LogRhythm for compliance

IT environments consist of heterogeneous devices, systems, and applications—all reporting log data. Millions of individual log entries can be generated daily, if not hourly. The task of organising this information can be overwhelming. Additional recommendations to analyse and report on log data render manual processes or homegrown remedies inadequate and cost prohibitive for many organisations.

LogRhythm delivers log collection, archiving, and recovery across the entire IT infrastructure and automates the first level of log analysis. Log data is categorised, identified, and normalised for easy analysis and reporting. LogRhythm’s powerful alerting capabilities automatically identify the most critical issues and notify relevant personnel. The KSA-ECC module and associated reporting package works out of the box with some level of customisation available. Utilising the KSA-ECC module assists in building and maintaining a sound compliance program.

Want to learn more about how LogRhythm can reduce your risk and time spent to demonstrate compliance? Visit www.logrhythm.com and request a demo today.