AUJAS CYBERSECURITY

NSE NSEIT

Saudi Arabia – National Cybersecurity Authority

# Essential Cybersecurity Controls (ECC – 1:2018) Standard Compliance

## Implementation Considerations

**Author:**
Tarun Ambwani, CISSP, CIPP
Vice President – Risk Advisory Services

## Introduction

Cyber-security is a complex and multifaceted challenge that is growing in importance. Traditionally viewed as an IT security problem, many organizations today realize that cyber security needs to be treated as a broader risk management issue to protect business interests against the adverse effects of cybercrime and hacktivism.

Cyber attacks are becoming more frequent, widespread and sophisticated. The rise in frequency and breadth of cyber attacks can be attributed to a number of factors:

- Unfriendly nation-states breach systems to seek intelligence or intellectual property.
- Hacktivists aim to make political statements through systems disruptions.
- Organized crime groups, cyber gangs, and other criminals breach systems for monetary gain—i.e., to steal funds via account takeovers, ATM heists, and other mechanisms.

As the cost of technology decreases, the barriers to entry for cyber crime drop, making it easier and cheaper for criminals of all types to seek out new ways to perpetrate cyber fraud.

In this paper, we aim to present some implementation considerations for Saudi Arabia's National Cybersecurity Authority Essential Cybersecurity Controls (ECC – 1:2018) Standard.

**United States:**
Tel: +1 408 973 7205

**Middle East:**
Tel: +971 6 5528438

**India:**
Tel: +91-80-2608 7878

**contact@aujas.com**

**www.aujas.com**

# I. Objective

The objective of this whitepaper is not to replicate the National Cybersecurity Authority's Essential Cybersecurity Controls (ECC – 1:2018) standard but to share our viewpoint on the important considerations that should be kept in mind while implementing the standard.

These implementation considerations can be used in conjunction with the ECC control text for elaborated guidance and also include recommendations that, while not required or explicitly mentioned in the ECC standard, are likely to add value to the implementation.

The whitepaper also includes a listing of the minimum set of documentation and evidences required for compliance to the standard.

# II. Introduction to NCA ECC Standard

The National Cybersecurity Authority of Saudi Arabia developed the Essential Cybersecurity Controls (ECC – 1: 2018) after conducting a comprehensive study of multiple national and international cybersecurity frameworks and standards, studying related national decisions, law and regulatory requirements, reviewing and leveraging cybersecurity best practices, analyzing previous cybersecurity incidents and attacks on government and other critical organizations, and surveying and considering opinions of multiple national organizations.

The Essential Cybersecurity Controls (ECC) consists of the following:

- 5 Cybersecurity Main Domains.
- 29 Cybersecurity Sub-domains.
- 114 Cybersecurity Controls.

### ECC Scope

These controls are applicable to government organizations in the Kingdom of Saudi Arabia (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), which are all referred to herein as "The Organization". The NCA strongly encourages all other organizations in the Kingdom to leverage these controls to implement best practices to improve and enhance their cybersecurity.

### ECC Applicability

These controls have been developed after taking into consideration the cybersecurity needs of all organizations and sectors in the Kingdom of Saudi Arabia. Every organization must comply with all applicable controls. Applicability to implement these cybersecurity controls depends on the organization's business and its use of certain technologies.

| | | | | |
|---|---|---|---|---|
| **Cybersecurity Governance** | 1-1 | Cybersecurity Strategy | 1-2 | Cybersecurity Management |
| | 1-3 | Cybersecurity Policies and Procedures | 1-4 | Cybersecurity Roles and Responsibilities |
| | 1-5 | Cybersecurity Risk Management | 1-6 | Cybersecurity in Information and Technology Project Management |
| | 1-7 | Compliance with Cybersecurity Standards, Laws and Regulations | 1-8 | Periodical Cybersecurity Review and Audit |
| | 1-9 | Cybersecurity in Human Resources | 1-10 | Cybersecurity Awareness and Training Program |
| **Cybersecurity Defense** | 2-1 | Asset Management | 2-2 | Cybersecurity Management |
| | 2-3 | Information System and Information Processing Facilities Protection | 2-4 | Cybersecurity Roles and Responsibilities |
| | 2-5 | Network Security Management | 2-4 | Cybersecurity in Information and Technology Project Management |
| | 2-7 | Data and Information Protection | 2-8 | Periodical Cybersecurity Review and Audit |
| | 2-9 | Backup and Recovery Management | 2-10 | Cybersecurity Awareness and Training Program |
| | 2-11 | Penetration Testing | 2-12 | Cybersecurity Event Logs and Monitoring Management |
| | 2-13 | Cybersecurity Incident and Threat Management | 2-14 | Physical Security |
| | 2-15 | Web Application Security | | |
| **Cybersecurity Resilience** | 3-1 | Cybersecurity Resilience Aspects of Business Continuity Management (BCM) | | |
| **Third Party and Cloud Computing Cybersecurity** | 4-1 | Third-Party Cybersecurity | 4-2 | Cloud Computing and Hosting Cybersecurity |
| **Industrial Control Systems Cybersecurity** | 5-1 | Industrial Control Systems (ICS) Protection | | |

# II. Important Considerations for NCA ECC Implementation

Prior to implementing the ECC standard, a detailed gap assessment should be conducted using the ECC assessment toolkit provided by NCA. Compliance to the ECC control should be supported by properly validated evidences.

The following considerations should not be interpreted as detailed implementation guidance covering all aspects of an ECC control. They are guidance statements that may be used as a supplementary to the ECC standard control text and also include value-add recommendations beyond the ECC standard control text.

## 1. Cybersecurity Governance

| Sub-domain | 1.1 Cybersecurity Strategy |
|---|---|
| Implementation Considerations | The cybersecurity strategy should be able to address both current business requirements and future growth plans that may result in IT/ICS/OT infrastructure changes or expansion. The strategy should be formulated after study of all potential solution options for cybersecurity keeping in mind advances in the cybersecurity space and also be able to address the organization's specific challenges.<br><br>The roadmap should identify all cybersecurity related focus areas, initiatives, high level action plans, and timeframes. A more detailed program plan for each focus area and its constituent initiatives can then be developed, executed, tracked and reported. |

| Sub-domain | 1.2 Cybersecurity Management |
|---|---|
| Implementation Considerations | The cybersecurity committee charter should include the committee mandate and objectives, authority, membership, roles and responsibilities, and governance framework. The latter can include the decision making model, baseline meeting agenda including owners, RACI matrix, any specialized processes, meeting frequency, participation and delegation. |

| Sub-domain | 1.3 Cybersecurity Policies and Procedures |
|---|---|
| Implementation Considerations | During the gap assessment stage, all existing policies and procedures should be reviewed to determine if all cybersecurity relevant areas are covered and adequately addressed. If gaps are found, these should be enhanced and where required additional policies or procedures should be defined, documented, approved, communicated, and implemented. |

| Sub-domain | 1.4 Cybersecurity Roles and Responsibilities |
|---|---|
| Implementation Considerations | A RACI matrix for key activities and roles involved may additionally be defined. |

| Sub-domain | 1.5 Cybersecurity Risk Management |
|---|---|
| Implementation Considerations | Common cybersecurity risks should be identified for all business departments/business processes in addition to identifying all security risks both technical and non-technical for IT/ICS/OT assets.<br><br>Additionally, while not required by the ECC, the cybersecurity risk management methodology can include an information security focused risk appetite. The risk appetite and methodology can be aligned with the enterprise and operational risk management methodology.<br><br>Further, implementation of a risk management technology solution for automation should be considered and it should be configured to provide a view of all enterprise wide risks as well as risk views by business departments, processes, facilities and assets. |

| Sub-domain | 1.6 Cybersecurity in Information and Technology Project Management |
|---|---|
| Implementation Considerations | While not required by ECC, the organization may additionally choose to automate project risk management via a technology solution. |

| Sub-domain | 1.7 Compliance with Cybersecurity Standards, Laws and Regulations |
|---|---|
| Implementation Considerations | A comprehensive compliance management framework must be in place including the overall compliance management process, procedures, reporting dashboards, roles and responsibilities, compliance requirements and controls library, compliance control checklists and questionnaires where applicable.<br><br>A unified compliance framework should be considered to reduce the number of compliance assessments. Integrated requirements or rationalization of requirements should be considered.<br><br>While not required by ECC, the organization may additionally choose to automate compliance management via a technology solution. |

| Sub-domain | 1.8 Periodical Cybersecurity Review and Audit |
|---|---|
| Implementation Considerations | Scope of the periodic independent reviews and audit should be carefully determined to include compliance reviews, security process area/control audits as well as technical security assessments. All core security processes and at-least all critical, high and other important assets (especially all external facing |

| | |
|---|---|
| | applications and perimeter devices as well as important internal applications) should be covered in the periodic technical assessment. Vendor rotation should be considered.<br>Remediation activities should be prioritized and completed on time. Where risk is being accepted, risk acceptance forms should be drafted with rationale and compensating controls and signed by the cybersecurity steering committee. |

| Sub-domain | 1.9 Cybersecurity in Human Resources |
|---|---|
| Implementation Considerations | The ECC control is clear. It is important to keep in mind that exiting personnel access to 'all information and technology assets must be permanently removed' via deletion of the user account and not just by disabling access. |

| Sub-domain | 1.10 Cybersecurity Awareness and Training Program |
|---|---|
| Implementation Considerations | The personnel targeted for cybersecurity awareness should cover all of the organization's staff including any third party contractors. It is recommended that all staff have access easy to awareness and training materials at all times e.g. via Intranet portal.<br>In addition, the organization may consider deploying a Learning Management System. While not required by ECC, the program may be extended to customers and partners. |

## 2. Cybersecurity Defense

| Sub-domain | 2.1 Asset Management |
|---|---|
| Implementation Considerations | A centralized up to date inventory (e.g. CMDB) of all information and technology assets (including hardware, software, applications, servers, databases, devices) must be maintained with relevant information for each that should include asset name, id, location, IP address, asset value or criticality level based on CIA, business department mapping, owner, custodian, among other parameters. |

| Sub-domain | 2.2 Identity and Access Management |
|---|---|
| Implementation Considerations | We recommend that multi-factor authentication for remote access be implemented on all customer facing applications as well as applications allowing remote access. In addition, we recommend that multi factor authentication should be implemented on administrator access to production environment.<br>The organization should consider implementing competent Identity Access |

| | |
|---|---|
| | Management and Privilege Access Management technology solutions.<br><br>Segregation of duties matrix for all applications must be developed and implemented. The same should be done for other IT assets such as servers, databases, network devices as well as security solutions. |

| Sub-domain | 2.3 Information System and Information Processing Facilities Protection |
|---|---|
| Implementation Considerations | Malware and virus protection should not only be restricted to the IT network but, if applicable, should be extended to other networks such as ATM. |

| Sub-domain | 2.4 Email Protection |
|---|---|
| Implementation Considerations | A detailed Email Security policy should be defined covering all points mentioned in the ECC control text as well as other requirements such as email usage policies, attachment handling, sharing of classified information over emails, email monitoring, etc. |

| Sub-domain | 2.5 Network Security Management |
|---|---|
| Implementation Considerations | In addition, Segregation of Duties (SOD) between the network and infrastructure management team (e.g. those managing servers, databases, routers, switches) as well as security device management team (e.g. those managing IDS/IPS, Firewalls, other security appliances/ solutions) should be defined, documented and implemented. Access control should be implemented in accordance to SOD, least privilege and need to know principles. |

| Sub-domain | 2.6 Mobile Devices Security |
|---|---|
| Implementation Considerations | A detailed Mobile Device Security and BYOD policy should be defined to capture other cybersecurity requirements such as not allowing jail-broken devices, restrictions on downloads and application installation, applying manufacturer provided security patches promptly when released, organization's applications being thoroughly tested for security flaws prior to their installation, etc. |

| Sub-domain | 2.7 Data and Information Protection |
|---|---|
| Implementation Considerations | It is recommended to define an overall Data Protection Governance framework including organization structure, roles and responsibilities, key activities and cross functional participation.<br><br>A Data and Information Protection Policy should be defined that is aligned with applicable legal, regulatory and industry standard requirements to include, but |

| | |
|---|---|
| | not limited to, areas such as: data ownership, data classification; data handling including collection, storage, use, transfer and disposal; media handling; and data protection. The policy, associated processes and procedures should be documented, approved and implemented.<br><br>A Data Classification, Handling and Protection Standard should be defined that describes based on the type of data and its classification and for each stage of collection, storage, use, transfer and disposal - how the data should be handled considering different data channels as well. |

| Sub-domain | 2.8 Cryptography |
|---|---|
| Implementation Considerations | A detailed cryptography policy in compliance with applicable laws, regulations and standards should be defined covering other areas such as where to use hardware vs software cryptography, digital certificate management, inventory of keys, assigning key custodians, annual review of the key inventory, logging and monitoring mechanism to detect key misuse or tampering, etc.<br><br>Conducting an assessment to move from less secure to more secure cryptographic implementation is recommended. For examples, on the implementation of cryptographic standards and ciphers for web services, it is preferred that TLS be used instead of SSL. If backward compatibility is required and supported by involved assets TLS 1.2 should be used. For new implementations where backward compatibility is not needed for communicating with other systems TLS 1.3 should be used. |

| Sub-domain | 2.9 Backup and Recovery Management |
|---|---|
| Implementation Considerations | A comprehensive backup and recovery management framework with roles and responsibilities, policies, processes, procedures, plans and schedules must be documented, approved and implemented.<br><br>While not explicitly mentioned in the ECC standard, from a cybersecurity requirement perspective, it is also recommended to annually assess controls implemented on data backup sites, physical repositories and systems for compromise risks and take remedial action. |

| Sub-domain | 2.10 Vulnerabilities Management |
|---|---|
| Implementation Considerations | While not required by or explicitly mentioned in the ECC standard, to add more effectiveness to the vulnerability management program: a compromise assessment using indicators of compromise can be conducted on a periodic basis to identify already compromised systems and take remedial action. |

| Sub-domain | 2.11 Penetration Testing |
|---|---|
| Implementation Considerations | In addition to Penetration Testing, Red Team Assessments can be considered. While the goal of penetration testing is to exploit known vulnerabilities and may or may not necessarily include identifying zero day vulnerabilities, the goal of the Red Team Assessment is to test the organization's detection and response capabilities by employing multiple targeted attack strategies and channels to gain access to sensitive information in an undetected way. |

| Sub-domain | 2.12 Cybersecurity Event Logs and Monitoring Management |
|---|---|
| Implementation Considerations | While the ECC control recommends monitoring only for critical assets, remote access and privileged user accounts, it is vital that the organization considers integration of all IT assets (including applications, databases, servers, devices) with the Security Information and Event Management (SIEM) solution for monitoring. Security solution integrations with the SIEM should be additionally considered.<br><br>A security event monitoring standard identifying all events to be monitored for an asset type or specific assets, where applicable, should be documented, approved and implemented. Logging policy and log levels should be clearly defined and implemented.<br><br>Additionally, developing tailored use cases for the SIEM solution, implementing correlation and conducting an exercise for evaluation the effectiveness of security monitoring and SIEM can be considered.<br><br>It is important to ensure that members of the security monitoring |

| Sub-domain | 2.13 Cybersecurity Incident and Threat Management |
|---|---|
| Implementation Considerations | A comprehensive cybersecurity incident management as well as threat management framework should be documented, approved and implemented. This should include a clear charter with organization structure, roles and responsibilities, and cross functional nvolvement for cybersecurity incident management and threat management. In addition incident management and threat management policy, process and procedures must be documented, approved, and implemented.<br><br>Other than threat feed integration into the Security Information and Event Management (SIEM) solution, a dedicated threat intelligence technology platform implementation may be considered to increase the coverage and quality of threat intelligence. Incident management should also include capability for rapid response and forensic investigation to deal with critical incidents.<br><br>Proactive gathering of threat intelligence, assessment of threat applicability, |

| | |
|---|---|
| | prompt communication of applicable threats to relevant stakeholders and their timely mitigation / resolution should be performed.<br><br>It is important to ensure that members of the threat and incident management staff are qualified and experienced to execute their assigned role. |

| Sub-domain | 2.14 Physical Security |
|---|---|
| Implementation Considerations | In addition, a physical security audit should be conducted at-least annually to determine the effectiveness of physical security practices, measures and controls. |

| Sub-domain | 2.15 Web Application Security |
|---|---|
| Implementation Considerations | While not explicitly mentioned in the ECC control text, it is recommended that threat profiling and subsequent remediation be done at a minimum for all external facing applications as well as other important applications. |

## 3. Cybersecurity Resilience

| Sub-domain | 3.1 Cybersecurity Resilience Aspects of Business Continuity Management |
|---|---|
| Implementation Considerations | At a minimum cybersecurity incident scenarios involving business critical application, systems and infrastructure should be defined and documented via collaboration between cyber incident response, business continuity management, disaster recovery and crisis management teams. Once these scenarios have been defined response plans including containment, contingency and recovery should be defined and documented by the group. Example scenarios may include Distributed Denial of Service Attacks, Ransomware Freeze, Zero Day Malicious Code Breakout, etc.<br><br>In addition, testing exercises to determine effectiveness of the response plan should be conducted. |

## 4. Third Party and Cloud Computing Cybersecurity

| Sub-domain | 4.1 Third-Party Cybersecurity |
|---|---|
| Implementation Considerations | The organization should perform both third party risk management (i.e. identifying risks introduced in their environment by engaging third parties) as well as third party due diligence prior to engaging third parties.<br><br>We recommend that the cybersecurity risk assessment for IT outsourcing and |

| | |
|---|---|
| | managed service providers conducted as part of due diligence not be limited to questionnaire based assessments rather the organization should obtain an independent report on the providers security, risk and compliance posture. The organization should additionally obtain written assurance from the provider as well as the independent third party who conducted the provider's assessment and/or audit that the report provided is factual, accurate, and complete. Alternatively, the organization may choose to appoint its own independent third party to perform the assessment and/or audit. Further, with such providers, the organization can include a right to any-time review or audit clause within the contractual agreement. |

| **Sub-domain** | **4.2 Cloud Computing and Hosting Cybersecurity** |
|---|---|
| **Implementation Considerations** | Cloud architecture review, cloud data access and data sharing review, cloud service provider contractual compliance keeping in mind applicable legal and regulatory requirements, as well as specialized cloud security assessment including process and technical risk assessment (e.g. vulnerability assessment, penetration testing, and configuration review) should be conducted. |

## 5. Industrial Control Systems Cybersecurity

| **Sub-domain** | **3.1 Cybersecurity Resilience Aspects of Business Continuity Management** |
|---|---|
| **Implementation Considerations** | Additionally, specialized penetration testing exercises for ICS and OT network and components can be considered. |

| ECC Subdomain | # | Minimum Documents and Evidences Required for Compliance |
|---|---|---|
| Cybersecurity Governance | 1 | Cybersecurity Strategy |
| | 2 | Cybersecurity Roadmap |
| | 3 | Cybersecurity Committee Charter |
| | 4 | Cybersecurity Governance Framework |
| | 5 | Cybersecurity Policies |
| | 6 | Cybersecurity Procedures |
| | 7 | Technical security standards/baselines |
| | 8 | Cybersecurity Organization Structure, Roles and Responsibilities |
| | 9 | Cybersecurity Risk Management Methodology |
| | 10 | Cybersecurity Risk Management Procedures |
| | 11 | Cybersecurity Requirements in Project Management |
| | 12 | Cybersecurity Requirements in Change Management |
| | 13 | Cybersecurity Requirements in Application Development |
| | 14 | List of Applicable Cybersecurity Laws, Regulations and Industry standards |
| | 15 | Compliance Management Framework, Process and Procedures |
| | 16 | Cybersecurity Compliance Requirements and Controls Library |
| | 17 | Cybersecurity Compliance Assessment, Tracking and Reporting Tool |
| | 18 | Cybersecurity Independent Audit and Review Reports |
| | 19 | Cybersecurity Requirements in Human Resources Process Document |
| | 20 | Cybersecurity Training and Awareness Framework Document |
| | 21 | Cybersecurity Training Plan and Materials |
| | 22 | Cybersecurity Awareness Plan and Materials |
| Cybersecurity Defense | 23 | Cybersecurity Requirements in Asset Management Policy and Process |
| | 24 | Acceptable Use Policy |
| | 25 | Information Classification Policy |
| | 26 | Cybersecurity Requirements in Identity and Access Management Policy |
| | 27 | Cybersecurity requirements for Protecting Information Systems and Information Processing Facilities |
| | 28 | Email Security Policy and Procedures |
| | 29 | Network Security Policy and Procedures |
| | 30 | Mobile Device Security Policy and Procedures |
| | 31 | BYOD Policy and Procedures |
| | 32 | Information Handling and Protection Standard |
| | 33 | Cryptography Policy |
| | 34 | Backup and Recovery Policy and Procedures |
| | 35 | Vulnerability Management and Penetration Testing Policy, Process and Procedure |

| ECC Subdomain | # | Minimum Documents and Evidences Required for Compliance |
|---|---|---|
| | 36 | Vulnerability Assessment and Penetration Testing ReportsCybersecurity Roadmap |
| | 37 | Security Monitoring Policy |
| | 38 | Event Monitoring Standard |
| | 39 | Incident Management Policy, Process and Procedures |
| | 40 | Threat Intelligence Policy, Process and Procedures |
| | 41 | Physical Security Policy |
| | 42 | Application Security Policy |
| **Cybersecurity Resilience** | 43 | Cybersecurity Requirements in Business Continuity Management |
| **Third Party and Cloud Computing Cybersecurity** | 44 | Cybersecurity Requirement in Third Party Management |
| | 45 | Cybersecurity Clauses in Third Party Contracts and Agreements |
| | 46 | Cybersecurity Requirements in Cloud Computing |
| | 47 | Cloud Computing Security Assessment Report |
| **Industrial Control Systems Cybersecurity** | 48 | Industrial Control Systems and Operational Technology Security Policy |
| | 49 | Industrial Control Systems and Operational Technology Security Procedures |
| | 50 | Industrial Control Systems and Operational Technology Security Assessment Reports |