VISTA INFOSEC®

TRUSTED ADVISORS, ASSURED COMPLIANCE™

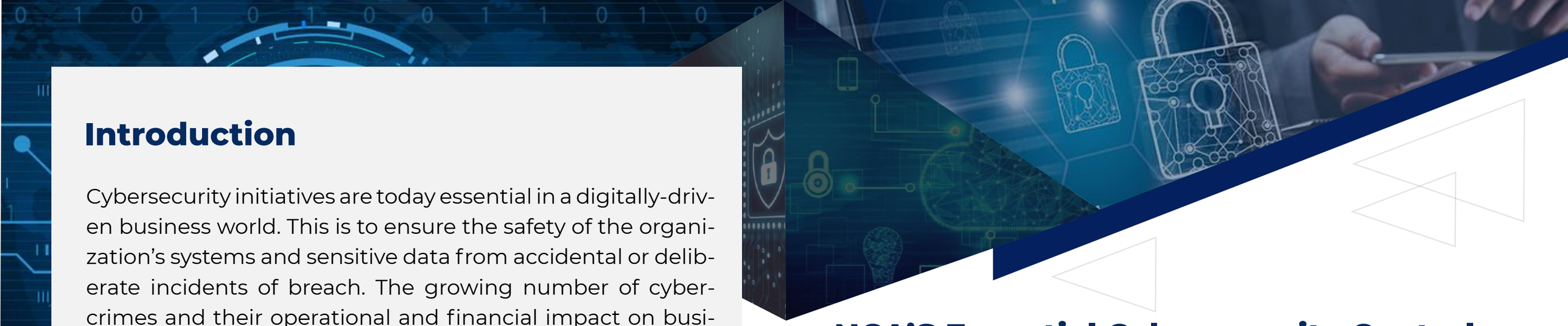
What is expected from organizations under NCA ECC Compliance?

W: www.vistainfosec.com | E: info@vistainfosec.com

US Tel: +1-415-513-5261 | UK Tel: +442081333131 | SG Tel: +65-3129-0397 | IN Tel: +91 73045 57744

An ISO27001 Certified Company, CERT-IN Empanelled, PCI QSA, PCI QPA and PCI SSFA

USA. SINGAPORE. INDIA. UK. MIDDLE EAST. CANADA.



Introduction

Cybersecurity initiatives are today essential in a digitally-driven business world. This is to ensure the safety of the organization's systems and sensitive data from accidental or deliberate incidents of breach. The growing number of cybercrimes and their operational and financial impact on business in terms of legal liability, reputational damage, and financial loss has pushed regulators to establish strong security measures and frameworks in place.

The urgent need to address cybersecurity threats has resulted in the adoption of industry best practices by regulators around the world. In 2018, Saudi Arabia's National Cybersecurity Authority (NCA) issued Essential Cybersecurity Controls (ECC) which is a minimum cybersecurity requirement for Saudi government organizations. The NCA encourages organizations in Saudi Arabia to adopt the ECC framework to improve their cybersecurity resilience.

Elaborating the framework and providing details on what is expected from organizations, we have in the article explained NCA's Essential Cybersecurity Controls.

NCA'S Essential Cybersecurity Controls

NCA ECC is a cybersecurity framework set for Saudi government organizations including ministries, authorities, establishments, and private sector organizations owning, operating, or hosting critical national infrastructure. The framework was established to improve cybersecurity efforts within the country. The ECC framework consists of 114 cybersecurity controls, linked to national and international regulatory requirements and defined into five main domains including cybersecurity governance, cybersecurity defense, cybersecurity resilience, third party, and cloud computing cybersecurity, and industrial control systems cybersecurity. Explaining each of the 5 domains and what is expected from the organization under these domains are all briefly described below

1. Cybersecurity Governance

Cybersecurity Strategy- The ECC's Cybersecurity Governance requires organizations to develop and implement cybersecurity strategies in line with relevant laws and regulations. The cybersecurity plans, goals, initiatives, and projects must facilitate compliance with related laws and regulations.

Cybersecurity Management- An independent Cybersecurity department must be established within the organization to ensure the implementation of the cybersecurity programs and initiatives within the organization. Along with the appointment of the cybersecurity function head who should be directly reporting to the head of the organization, roles and responsibilities and governance framework must be defined, documented, and approved within the organization.

Cybersecurity Policies & Procedures- The organization must have documented policies and procedures in place that ensures the enforcement of laws and regulation within the organization. The policies and procedures established must be supported by technical security standards and must be reviewed periodically according to the planned intervals or upon changes to related laws and regulations.

Cybersecurity Roles & Responsibilities - The roles and responsibilities related to cybersecurity must be defined, documented, approved, supported, and assigned by the Authorizing Official while ensuring no conflict of interest. The roles and responsibilities must be also periodically reviewed based on the planned intervals or upon changes to related laws and regulations.

Cybersecurity Risk Management- The organization is expected to adopt a methodological approach to protect the organization's information and technology assets as per organizational policies and procedures and which should be in line with the regulations. The Risk Management approach must be defined, documented, and approved as per confidentiality, integrity, and availability considerations of information and technology assets and must be implemented by cybersecurity functions.

Cybersecurity Policies & Procedures- The organization must have documented policies and procedures in place that ensures the enforcement of laws and regulation within the organization. The policies and procedures established must be supported by technical security standards and must be reviewed periodically according to the planned intervals or upon changes to related laws and regulations.

Cybersecurity Roles & Responsibilities -The roles and responsibilities related to cybersecurity must be defined, documented, approved, supported, and assigned by the Authorizing Official while ensuring no conflict of interest. The roles and responsibilities must be also periodically reviewed based on the planned intervals or upon changes to related laws and regulations.

Cybersecurity Risk Management- The organization is expected to adopt a methodological approach to protect the organization's information and technology assets as per organizational policies and procedures and which should be in line with the regulations. The Risk Management approach must be defined, documented, and approved as per confidentiality, integrity, and availability considerations of information and technology assets and must be implemented by cybersecurity functions.

Cybersecurity in Information and Technology Project Management- Organizations must consider cybersecurity requirements in their Project Management Methodology and procedures to protect the confidentiality, integrity, and availability of Information and Technology Assets. The requirements must essentially be a part of the overall requirements of Information and Technology projects.

Compliance with Cybersecurity Standards, Laws, and Regulations- The organization's cybersecurity program must be aligned with the cybersecurity standards, laws, and regulations.

Periodical Cybersecurity Review and Audit- The organization's cybersecurity program must be aligned with the cybersecurity standards, laws, and regulations.

Further, Cybersecurity audits and reviews must be conducted by independent parties outside the cybersecurity function to ensure no conflict of interest, as per the Generally Accepted Auditing Standards (GAAS), and related laws and regulations.

Cybersecurity in Human Resources- Organizations must consider cybersecurity in their human resource management initiatives especially before employment, during employment, and after termination/separation as per organizational policies and procedures. This should include communicating cybersecurity responsibilities, non-disclosure clauses, organizational policies and procedures pertinent to cybersecurity, and conducting Cybersecurity awareness programs.

Cybersecurity Awareness and Training Program- Organizations are expected to conduct regular Cybersecurity Awareness and Training programs for their employees. This is to ensure that the employees are aware of their responsibilities and have the essential knowledge and awareness of cybersecurity measures.

2. Cybersecurity Defence

Asset Management - Organizations are expected to maintain an accurate and detailed inventory of information and technology assets to support the organization's cybersecurity and operational requirements and maintain the confidentiality, integrity, and availability of information and technology assets.

Identity and Access Management - Organizations are expected to maintain secure and restricted logical access to information and technology assets to prevent unauthorized access and allow only authorized access for users which are necessary to accomplish assigned tasks. Necessary cybersecurity requirements should be implemented for identity and access management and the same should be reviewed periodically.

Information System and Information Processing Facilities Protection - Organizations must implement relevant and necessary security measures to protect information systems and information processing facilities against cyber risks.

The implemented measures must be defined, documented, approved, and even reviewed periodically.

Email Protection - Organizations must define document and approve the Cybersecurity requirements to be implemented for protecting email services. This should include Analysing and filtering of email, Multi-factor authentication for remote and webmail access, email archives and backups, etc.

Networks Security Management - Organizations should implement network segmentation/segregation to secure the organization's network against cyber threats. They are required to implement various cybersecurity requirements including Logical or physical segregation and segmentation of network segments, Secure browsing and Internet connectivity, strong authentication of wireless networks, Intrusion Prevention Systems (IPS), Security of Domain Name Service (DNS), security measures against Advanced Persistent Threats (APT) to name a few. The implemented security measures must be reviewed periodically necessary measures are in place and in alignment with the evolving threats.

Mobile Device Security - Organizations are required to protect all mobile devices against cyber threats and ensure the secure handling of all sensitive information under their Bring Your Own Device policy (BYOD). The cybersecurity requirements for mobile devices must include Separation and encryption of the organization's data, Controlled and restricted use of mobile devices, and Secure wiping of data in cases of device loss, theft, or after termination/separation.

Data and Information Protection - Organizations must implement security measures and ensure the confidentiality, integrity, and availability of the organization's data and information as per organizational policies and procedures, and related laws and regulations. The implemented measures must be reviewed periodically.

Cryptography - Organizations must define, document, and approve measures to implement cryptography. This is to ensure the proper and efficient use of cryptography to protect information assets as per organizational policies and procedures, and related laws and regulations.

Backups and Recovery Management - Organizations must ensure the protection of the organization's data and information including information systems and software configurations from cyber risks. The organization must accordingly define, document, approve and implement backup and recovery management and test the same for its effectiveness.

Vulnerability Management - Organizations must conduct a periodic vulnerability assessment to ensure timely detection and remediation of vulnerabilities. This is to prevent and minimize the risk of cyber-attacks due to the exploitation of unidentified vulnerabilities.

Penetration Testing - Organizations must simulate cyber-attacks to discover unknown weaknesses within the technical infrastructure that may result in cyber-breach. This is to assess and evaluate the efficiency of the organization's cybersecurity defense capabilities. The penetration testing exercises must be defined, documented, approved, and periodically performed.

Cybersecurity Event Logs and Monitoring Management - Organizations must have in place Cybersecurity event logs and monitoring management systems for early detection of anomalies. This is to prevent or minimize the impact of the incident on the organization. Organizations are expected to activate cybersecurity event logs on critical information assets and remote access, and privileged user accounts, while also constantly monitor event logs and retain the records for 12 months.

Cybersecurity Incident and Threat Management - Organizations are expected to have in place an Incident Response and Management system to quickly take necessary measures in case of an incident. This is to minimize the damage caused due to the incident that occurred and its impact on the organization's operations.

Physical Security - Organizations must implement physical security measures to protect the information and technology assets of the organization. The measures implemented must be defined, documented, and approved. The physical protection implemented must include restricting access to sensitive facilities, CCTV monitoring at entry and exits, secure destruction and re-use of physical assets holding classified information, Security of devices and equipment comprising sensitive data.

Web Application Security - Organizations are expected to implement security measures for web applications to ensure protection against various cyber risks. The cybersecurity requirements for external web applications must include the use of a web application firewall, use of secure protocols, multi-factor authentication for users' access, adoption of the multi-tier architecture principle, and establishing a secure usage policy for users. Organizations must also periodically review the cybersecurity requirements for external web applications.

3. Cybersecurity Resilience

Organizations must ensure the inclusion of the cybersecurity resiliency requirements within the organization's Business Continuity Management to remediate and minimize the impacts on systems, information processing facilities, and critical e-services from disasters caused by cybersecurity incidents. This would include having in place Incident Response Plans and Disaster Recovery Plans which must also be reviewed periodically.

4. Third-Party and Cloud Computing Cybersecurity

Third-Party Cybersecurity - In terms of third-party risks, organizations are expected to have in place policies, procedures ensuring the security of outsourced services. This should include having in place contracts and agreements with the third party that must be documented and approved. The contract or agreement documents must communicate disclosure policy, procedures in case of cybersecurity incidents, and requirements to comply with related organizational policies and procedures, laws, and regulations.

Cloud Computing and Hosting Cybersecurity - The organizations must implement cybersecurity measures for hosting and cloud computing which should be aligned with the organizational policies and procedures, and related laws and regulations. The implemented measures must be defined, documented, and approved. The cybersecurity requirements related to hosting and cloud computing services must be reviewed periodically.

5. Industrial Control System Cybersecurity

Industrial Control Systems (ICS) Protection - Cybersecurity requirements related to Industrial Controls Systems and Operational Technology (ICS/OT) must be defined, documented approved, and implemented. The implementation of measures must include physical and virtual segmentation when connecting industrial production networks to other networks within the organization and networks to other networks within the organization and external networks. Other measures required to be implemented should include Continuous monitoring and activation of event logs, Isolation of Safety Instrumental Systems, limitation on connecting mobile devices to industrial production networks, limitation on the use of external storage media, patch management, vulnerability management, cybersecurity application management and periodic review of all measures implemented.

How can VISTA InfoSec help with NCA ECC Compliance?

VISTA InfoSec is a global cybersecurity consulting firm having nearly two decades of presence in the industry.

With combined expertise, knowledge, and experience in the industry, our team of in-house experts can assist you in your journey of compliance and help you implement the required security measures and controls for achieving compliance.

Our solutions and advisory services are particularly effective with regards to implementing some of the identified controls outlined by the **NCA.**

We help you translate these requirements into a systematic implementation process and ensure security and Compliance to **NCA's ECC.**

Contact Us

US Tel: +1-415-513-5261 | UK Tel: +442081333131

SG Tel: +65-3129-0397 | IN Tel: +91 73045 57744

www.vistainfosec.com

info@vistainfosec.com