This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. Items highlighted in green are examples and should be removed. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the placeholder to the left.

Cybersecurity Requirements Checklist for Software Development Template

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press “Ctrl” + “H” keys simultaneously.
- Enter “<organization name>” in the Find text box.
- Enter your organization’s full name in the “Replace” text box.
- Click “More”, and make sure “Match case” is ticked.
- Click “Replace All”.
- Close the dialog box.

Choose Classification

DATE	Click here to add date
VERSION	Click here to add text
REF	Click here to add text

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual's full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated By	Version Details
<Insert version number>	Click here to add date	<Insert individual's full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Purpose

This checklist aims to define the cybersecurity requirements for software development activities in <organization name>. The ability of <organization name> to implement the requirements in accordance with this checklist will assist in the development and release of secure software for end users and in preserving the availability, integrity and confidentiality of <organization name>'s assets and information.

The requirements in this checklist are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) including but not limited to ECC-١:٢٠١٨, in addition to other related cybersecurity legal and regulatory requirements.

Scope

The checklist covers <organization name>'s cybersecurity requirements in software development and applies to all personnel (employees and contractors) in <organization name>.

Requirements

The following table should be filled in by <organization name> in order to document the implementation of cybersecurity requirements in the software development process. A description of each column in this table is provided in Appendix A.

Cybersecurity requirements checklist for software development								
Id	**Activity**	**Description**	**Mandatory**	**Phase**	**Status**	**Implementation deadline**	**Comment**	**Evidence**
١	Software Assets Registration	Centralized repository was set up and used to store all information related to the project.	Yes	Plan	Choose status.	Choose date.		
٢	Development tool stack	Centralized solution for source code tracking and artifacts processing, release and deployment were in place allowing for automatic deployment to environment and cybersecurity controls deployment.	Yes	Plan	Choose status.	Choose date.		
٣	Threat Modeling Analysis	Threat modeling for developed application was performed, allowing for proper risks and requirements	Yes	Plan	Choose status.	Choose date.		

Cybersecurity requirements checklist for software development								
Id	**Activity**	**Description**	**Mandatory**	**Phase**	**Status**	**Implementation deadline**	**Comment**	**Evidence**
		identification.						
٤	Regulatory / Internal Compliance	Evaluation for external (legal and regulatory) and internal requirements was conducted and derived requirements were considered in designing cybersecurity controls.	Yes	Plan	Choose status.	Choose date.		
٥	Application Risk Profiling	Evaluation of cybersecurity risks of the application was conducted in line with cybersecurity risk management standard to identify potential business impact in case of any cybersecurity risk materializing.	Yes	Plan	Choose status.	Choose date.		

Cybersecurity requirements checklist for software development								
Id	**Activity**	**Description**	**Mandatory**	**Phase**	**Status**	**Implementation deadline**	**Comment**	**Evidence**
٦	Security Requirements Definition	Cybersecurity requirements, derived from functional requirements and previous activities (Threat Modeling Analysis, Regulatory/internal compliance, Application Risk Profiling) were defined.	Yes	Plan	Choose status.	Choose date.		
٧	Definition of Groups and Roles	Prior to the development activities, roles and responsibilities were defined, to ensure least privileges principle. The following factors were taken into account: - Environment type - Access to development tools, Continuous Integration/Continuous Delivery pipelines - Sensitivity of data used for development	Yes	Governance	Choose status.	Choose date.		

Cybersecurity requirements checklist for software development								
Id	**Activity**	**Description**	**Mandatory**	**Phase**	**Status**	**Implementation deadline**	**Comment**	**Evidence**
٨	Security Champion Definition	An intermediary between the cybersecurity department and development teams was defined to ensure communication of requirements and knowledge exchange as well as solving issues arising during development.	Yes	Governance	Choose status.	Choose date.		
٩	Issues Management	Centralized repository of issues raised was used during development. It was capable to ingest and track following items: - Unmet requirements - Security weaknesses raised during testing - Other cybersecurity related observations	No	Governance	Choose status.	Choose date.		

Cybersecurity requirements checklist for software development								
Id	**Activity**	**Description**	**Mandatory**	**Phase**	**Status**	**Implementation deadline**	**Comment**	**Evidence**
١٠	Security Gates Definition	Mandatory checkpoints and corresponding requirements for proceeding of the development process were defined. These control points help to determine whether implemented security controls sufficiently address identified cybersecurity risks.	Yes	Governance	Choose status.	Choose date.		
١١	Environments Separation	At minimum Development, Testing and Production environments were set up. Developer access to the production environment was provided for limited time only and under supervision.	Yes	Governance	Choose status.	Choose date.		

Cybersecurity requirements checklist for software development								
Id	**Activity**	**Description**	**Mandatory**	**Phase**	**Status**	**Implementation deadline**	**Comment**	**Evidence**
١٢	Testing Data Sanitization	Data used for testing derived from production data was sanitized and sensitive data was replaced with random content.	Yes	Governance	Choose status.	Choose date.		
١٣	Third Party Components Approval	All third party components were already assessed by the cybersecurity team and approved for use in the development process. Scope of the assessment included verification of resilience against cybersecurity attack, licensing model, and compliance with regulatory requirements.	Yes	Governance	Choose status.	Choose date.		
١٤	SLA Definition	Service Level Agreement (SLA) for addressing issues raised during development was defined and tracked during the	Yes	Governance	Choose status.	Choose date.		

Cybersecurity requirements checklist for software development								
Id	**Activity**	**Description**	**Mandatory**	**Phase**	**Status**	**Implementation deadline**	**Comment**	**Evidence**
		development process.						
١٥	Metrics Management	Metrics collected during development were tracked and eventual remediation activities conducted in case when aberrations from SLAs were detected.	Yes	Governance	Choose status.	Choose date.		
١٦	Team Training	Development teams and other personnel involved in the process were trained and had current knowledge related to cybersecurity risks in software development as well as corresponding activities implemented in the organization.	Yes	Governance	Choose status.	Choose date.		

Cybersecurity requirements checklist for software development								
Id	**Activity**	**Description**	**Mandatory**	**Phase**	**Status**	**Implementation deadline**	**Comment**	**Evidence**
١٧	Secure Development Guidelines	Guidelines on secure usage of technologies used in the development process were created and up-to-date and used by the team.	Yes	Code	Choose status.	Choose date.		
١٨	IDE Static Analysis	Code editors used for development were integrated with solutions which statically assess compliance against cybersecurity guidelines. Results of such analysis were used to determine whether code quality from a cybersecurity perspective is adequate to commit the code to a centralized repository.	No	Code	Choose status.	Choose date.		

Cybersecurity requirements checklist for software development								
Id	**Activity**	**Description**	**Mandatory**	**Phase**	**Status**	**Implementation deadline**	**Comment**	**Evidence**
١٩	Static Application Security Testing (SAST)	Automatic static application security testing was conducted based on a risk assessment and determined application classification. Results were tracked and addressed accordingly to agreed SLAs; prior to scanning, fine tuning of scanner configuration was conducted to ensure that the entire code base is reviewed for security flaws.	No	Test	Choose status.	Choose date.		
٢٠	SCA	Automatic software composition analysis was conducted to determine whether all components used for building the application are free of vulnerabilities and are used in the proper way.	No	Test	Choose status.	Choose date.		

Cybersecurity requirements checklist for software development								
Id	**Activity**	**Description**	**Mandatory**	**Phase**	**Status**	**Implementation deadline**	**Comment**	**Evidence**
٢١	Configuration Review	Automatic assessment of configuration parameters of components used in development and production environments against current, approved hardening guides for each technology was conducted, including, but not limited to: - security architecture - operating systems - databases - middleware - containers - external service providers - cloud resources	Yes	Test	Choose status.	Choose date.		

Cybersecurity requirements checklist for software development								
Id	**Activity**	**Description**	**Mandatory**	**Phase**	**Status**	**Implementation deadline**	**Comment**	**Evidence**
٢٢	DAST	Automatic dynamic application security testing was conducted based on a risk assessment and determined application classification. Results were tracked and addressed accordingly to agreed SLAs; prior to scanning, fine tuning of scanner configuration was conducted to ensure that the entire code base is reviewed for security flaws (including configuration of authentication and authorization).	No	Test	Choose status.	Choose date.		

Cybersecurity requirements checklist for software development								
Id	**Activity**	**Description**	**Mandatory**	**Phase**	**Status**	**Implementation deadline**	**Comment**	**Evidence**
٢٣	Penetration Testing	Manual dynamic application security testing was conducted based on a risk assessment and determined application classification. Results were tracked and addressed accordingly to agreed SLAs; prior to scanning, fine tuning of scanner configuration was conducted to ensure that the entire code base is reviewed for security flaws (including configuration of authentication and authorization).	No	Test	Choose status.	Choose date.		

Cybersecurity requirements checklist for software development								
Id	**Activity**	**Description**	**Mandatory**	**Phase**	**Status**	**Implementation deadline**	**Comment**	**Evidence**
٢٤	Security Monitoring	Applications deployed in the production environment was monitored for security incidents, known patterns and any anomalies which might indicate novel attacks. Monitoring included application, system, middleware and cloud events. Incident Response procedure and application catalog were set up to date and included newly deployed applications.	Yes	Operate	Choose status.	Choose date.		
٢٥	Endpoint Security	Endpoints used in the application runtime environment met <organization name> hardening requirements.	Yes	Endpoint security	Choose status.	Choose date.		

Cybersecurity requirements checklist for software development								
Id	**Activity**	**Description**	**Mandatory**	**Phase**	**Status**	**Implementation deadline**	**Comment**	**Evidence**
٢٦	Business Continuity	Application was assessed from a Business Continuity perspective ensuring processes and controls were updated to include newly deployed components.	Yes	Infrastructure security	Choose status.	Choose date.		
٢٧	Asset Management	All newly developed components were onboarded via Asset Management system tracked for any changes.	Yes	Infrastructure security	Choose status.	Choose date.		
٢٨	Configuration Management	Configuration of all components were tracked for unauthorized changes and complete approval path was stored, in line with organization's Change Management procedure.	Yes	Infrastructure security	Choose status.	Choose date.		

Cybersecurity requirements checklist for software development								
Id	**Activity**	**Description**	**Mandatory**	**Phase**	**Status**	**Implementation deadline**	**Comment**	**Evidence**
٢٩	Vulnerability Management	Application components were included in regular vulnerability scan scope and resulting observations were handled using already established procedures as part of <organization name> Vulnerability Management policy.	Yes	Operate	Choose status.	Choose date.		
٣٠	Integration with Security Services	Production environment was integrated with available security services (depending on classification) including, but not limited to: - Intrusion Prevention/Detection System - Web Application Firewall - Endpoint Detection Response System - Security Information and Evidence Management	Yes	Operate	Choose status.	Choose date.		

Cybersecurity requirements checklist for software development								
Id	**Activity**	**Description**	**Mandatory**	**Phase**	**Status**	**Implementation deadline**	**Comment**	**Evidence**
		system						
٣١	Secrets Management	Configuration parameters including sensitive values (i.e., credentials keys, certificates, license keys, etc.) were rotated and modified from the ones used in development. Secrets were stored in a safe way, using mechanisms available in the platform in place. Processes were in place to ensure that secrets are rotated periodically and securely disposed of.	Yes	Operate	Choose status.	Choose date.		

Cybersecurity requirements checklist for software development								
Id	**Activity**	**Description**	**Mandatory**	**Phase**	**Status**	**Implementation deadline**	**Comment**	**Evidence**
٣٢	Threat Intelligence	Application was included in regular Threat Intelligence activities and necessary changes were applied to application and runtime environments in response to arising threats.	Yes	Operate	Choose status.	Choose date.		

Roles and Responsibilities

١- **Checklist Owner:** <head of the cybersecurity function>

٢- **Checklist Review and Update:** <cybersecurity function>

٣- **Checklist Implementation and Execution:** <Information Technology function>

٤- **Checklist Compliance Measurement**: <cybersecurity function>

Update and Review

<cybersecurity function> must review the checklist at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

١- The <head of the cybersecurity function> will ensure compliance of <organization name> with this checklist on a regular basis.

٢- All personnel at <organization name> must comply with this checklist.

٣- Any violation of this checklist may be subject to disciplinary action according to <organization name>'s procedures.

Appendix A – Checklist column name description

Legend	
Column name	**Description**
Id	*Identification number assigned to the activity*
Activity	*Name of the activity to be completed*
Description	*Description of the activity to be completed*
Mandatory	*Is the particular control required or can be omitted on the condition that it is not viable to implement, and security team approves it*
Phase	*Phase assigned to the activity to be completed*
Status	*Information on control implementation status, possible states:* ➢ *Completed* ➢ *In progress* ➢ *Not applicable*
Implementation deadline	*Date by which the control must be implemented and status change to Completed or Not applicable*
Comment	*Additional note on the control implementation status*
Evidence	*Information on it how the requirement has been handled - screenshot or link to documentation*