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 IT Projects and Change Management Template

Choose Classification

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

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.

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 defines the minimum cybersecurity requirements related to IT Projects and Change Management for <organization name>. The ability of <organization name> to implement the requirements in accordance with this checklist will assist in mitigating cybersecurity risks in IT Projects and Change Management 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-1:2018, in addition to other related cybersecurity legal and regulatory requirements.

Scope

The checklist covers <organization name>'s cybersecurity requirements in IT Projects and Change Management and applies to all personnel (employees and contractors) in <organization name>.

Requirements

The following table should be filled in by <organization name>'s Project Manager to document implementation of cybersecurity controls in the IT Project or Change Management process.

IT Projects and Change Management Cybersecurity Requirements checklist											
					Change type						
Id	Activity name	Description	Mandatory	Phase	Planned change	Project	Emergency change	Status	Implementation deadline	Comment	Evidence
1	Stakeholder Identification Management	Relevant stakeholders were appointed and involved in the project/change including but not limited to team members responsible for; • managerial oversight over this engagement • project management in this engagement • cybersecurity matters in this engagement • solutions impacted by this engagement • risk management • implementing the change	Yes	Stakeholder identification	x	x		Choose status.	Choose date.		
2	Documentation Retention	All documentation and communication regarding project/change was stored in a location accessible by authorized personnel only and all data was	Yes	Initiation	x	x	x	Choose status.	Choose date.		

IT Projects and Change Management Cybersecurity Requirements checklist											
		archived in line with data retention policy.									
3	Change Classification	The change was classified either as a planned change, IT project or emergency change.	Yes	Initiation	x	x	x	Choose status.	Choose date.		
4	Impact Assessment	Impact of the change was assessed and the results must drive the execution decision and definition of cybersecurity controls to be implemented.	Yes	Initiation	x	x	x	Choose status.	Choose date.		
5	Vendor Assessment	If a third party vendor was involved in the project, vendor assessment was conducted in line with the internal process, including but not limited to third party cybersecurity risk assessment and security background check.	Yes	Initiation		x		Choose status.	Choose date.		

IT Projects and Change Management Cybersecurity Requirements checklist											
6	Threat Modeling Analysis	Threat modeling for the project must be performed, allowing for proper risks and requirements identification.	Yes	Initiation		x		Choose status.	Choose date.		
7	Regulatory / Internal Compliance	Evaluation for external (legal and regulatory) and internal requirements was conducted and derived requirements were considered in designing cybersecurity controls.	Yes	Initiation		x		Choose status.	Choose date.		
8	Project Risk Profiling	Evaluation of cybersecurity risks of the project/change was conducted in line with cybersecurity risk management standard to identify potential business impact in case of any cybersecurity risk materializing.	Yes	Initiation		x		Choose status.	Choose date.		
9	Security Requirements Definition	Cybersecurity requirements, derived from functional requirements and previous activities (Threat Modeling Analysis, Regulatory/internal compliance, Application Risk Profiling) were defined.	Yes	Initiation	x	x		Choose status.	Choose date.		

IT Projects and Change Management Cybersecurity Requirements checklist											
10	Software Development	In case custom software development was conducted, "Software Development Cybersecurity Checklist" was prepared and followed.	Yes	Implementation		x		Choose status.	Choose date.		
11	Asset Management	All newly developed components were onboarded via Asset Management tool and tracked for any changes.	Yes	Implementation	x	x		Choose status.	Choose date.		
12	Testing	Change was tested prior to implementation in the production environment. Test cases included assessment for the presence of cybersecurity related vulnerabilities. Scope of the testing was tailored for the extent of the change, and at minimum included vulnerability scanning.	Yes	Release	x	x	x	Choose status.	Choose date.		
13	Simulation	Testing environment simulated the production one to the extent possible, and all differences were accounted for and approved.	Yes	Release	x	x	x	Choose status.	Choose date.		

IT Projects and Change Management Cybersecurity Requirements checklist											
14	Release signoff	All relevant stakeholders signed off the change before release to the production, confirming that all prerequisites have been provided, including successful testing, and addressing identified risks.	Yes	Release	x	x		Choose status.	Choose date.		
15	Final signoff	All stakeholders signed off the change after release to the production, confirming that change was implemented successfully in production and all requirements have been met.	Yes	Release	x	x		Choose status.	Choose date.		
16	Change Implementation Monitoring	Change was tracked and consulted with stakeholders on a regular basis after implementation and evidence for consultation was stored for future reference.	Yes	Operations	x	x	x	Choose status.	Choose date.		
17	Reevaluation of Emergency Change	Emergency change was reassessed either as change or project as soon as possible, and additional requirements was fulfilled.	Yes	Release			x	Choose status.	Choose date.		

Roles and Responsibilities

1- **Checklist Owner:** <head of the cybersecurity function>
2- **Checklist Review and Update:** <cybersecurity function>
3- **Checklist Implementation and Execution:** <Information Technology function>
4- **Checklist Compliance Measurement**: <cybersecurity function>

Update and Review

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

Compliance

1- The <head of the Cybersecurity function> will ensure compliance of <organization name> with this checklist on a regular basis.
2- All personnel at <specific IT function name> at <organization name> must comply with this checklist.
3- Any violation of this checklist may be subject to disciplinary action according to <organization name>'s procedures.