CyFun® 2025 – Group-Context Application Guidance

Purpose

This annex explains how an entity within a larger organisation demonstrates conformity to CyFun® 2025[1] where governance, strategy, and cyber risk management are defined at group level and cascade to the entity.

Applicability Model

CyFun® 2025 controls may be applied in a group context as follows:

- Inherited: Controls whose governance, decision making, and assurance are exercised at the group level, and which the entity formally relies on (or adopts).
- Implemented: Controls governed through group defined standards but (implemented) executed, overseen, and assured through the entities own governance structures.
- Shared: Responsibilities are split between the group and the entity.

Regardless of the application model, the entity remains accountable for demonstrating effective application of applicable CyFun® 2025 controls within its scope.

Domain-by-domain application of CyFun® 2025 controls in a group context

The following sections describe how CyFun® 2025 control families typically apply to entities that are part of a larger organisation.

GOVERN (GV)

Applicable control families:

- GV.OC – Organisational Context
- GV.RM – Risk Management Strategy
- GV.RR – Roles, Responsibilities and Authorities
- GV.PO – Policy
- GV.OV – Oversight
- GV.SC – Cybersecurity Supply Chain Risk Management

Controls in the GOVERN domain are typically defined and coordinated at group level. The entity demonstrates conformity by formally adopting group governance, policies and risk management frameworks, establishing local roles and reporting lines aligned with the group structure, and applying group-defined oversight and supply-chain requirements within its own scope. The entity is not required to redefine governance arrangements but remains accountable for their effective application.

[1] Until the end of the transition period (see cyfun.eu), this document also applies to CyFun®2023.

CyFun® 2025 – Group-Context Application Guidance

IDENTIFY (ID)

Applicable control families:

- ID.AM – Asset Management
- ID.RA – Risk Assessment
- ID.IM – Improvement

Controls in the IDENTIFY domain are primarily implemented at entity level using group-defined methods and tools. The entity demonstrates conformity by maintaining accurate inventories of assets, services, data and suppliers, performing risk assessments using the group methodology, and ensuring that changes in its context are reflected in inventories, risk assessments and improvement activities.

PROTECT (PR)

Applicable control families:

- PR.AA – Identity, Authentication and Access Control
- PR.AT – Awareness and Training
- PR.DS – Data Security
- PR.PS – Platform Security
- PR.IR – Technology Infrastructure Resilience

Controls in the PROTECT domain are generally shared. Group-defined security policies, standards and technologies are implemented locally by the entity. The entity demonstrates conformity by ensuring effective coverage of its systems and services, ensuring personnel participate in required training, and managing documented exceptions where necessary.

DETECT (DE)

Applicable control families:

- DE.CM – Continuous Monitoring
- DE.AE – Adverse Event Analysis

Controls in the DETECT domain are typically operated centrally at group level. The entity demonstrates conformity by ensuring that its systems and services are within scope of group monitoring capabilities, by defining local alert-handling and escalation responsibilities, and by acting on detection outputs relevant to its environment.

RESPOND (RS)

Applicable control families:

- RS.MA – Incident Management
- RS.AN – Incident Analysis
- RS.CO – Incident Communication
- RS.MI – Incident Mitigation

Controls in the RESPOND domain are coordinated at group level and executed jointly. The entity demonstrates conformity by participating in group incident response processes, executing defined local response and containment actions, and contributing entity-specific information to incident analysis and improvement.

RECOVER (RC)

Applicable control families:

- RC.RP – Incident Recovery Plan Execution
- RC.CO – Recovery Communication

Controls in the RECOVER domain are shared between the group and the entity. The entity demonstrates conformity by aligning its recovery arrangements with group business continuity and disaster recovery frameworks, meeting defined recovery objectives for its critical services, and participating in testing and recovery-related communications.

CyFun® 2025 control maturity scoring in a group context

Core rule

Maturity level reflects how well a control is documented, implemented, measured and improved for the entity, regardless of whether that control is defined at group or entity level. An entity may achieve any CyFun® 2025 maturity level using group defined controls, provided that documentation is formally applicable and implementation evidence and metrics exist at entity level.

Mapping between control applicability and maturity dimensions

Control Type*	Documentation Maturity	Implementation Maturity
Inherited	Group documentation formally applicable to the entity	Effective and consistent use within the entity's scope
Implemented	Entity documentation	Entity implementation
Shared	Group documentation + entity supplements	Joint operation + entity execution

* See Applicability Model

How to score maturity per level for group-context controls

Below is a practical interpretation of each maturity level that works uniformly for Inherited, Shared, and Implemented controls.

CyFun® 2025 – Group-Context Application Guidance

Level 1 – Initial

Documentation

- No applicable group or entity documentation
  OR
- Documentation exists but is not formally approved or applicable to the entity

Implementation

- No standard group process covering the entity
- Entity actions are ad hoc or absent

Level 2 – Repeatable

Documentation

- Group or entity documentation exists and is formally approved
- Documentation applies to the entity
- Documentation has not been reviewed in the last 2 years

Implementation

- Group process exists
- Entity follows it informally or inconsistently

Level 3 – Defined

Documentation

- Group documentation:
  - formally approved
  - applicable to the entity
  - exceptions documented and approved
- Entity-specific deviations documented
- Exceptions < 5%

Implementation

- Standard group process is implemented
- Evidence exists for most entity activities
- Exceptions < 10%

Level 4 – Managed

Documentation

- Group documentation:
  - formally approved
  - applicable
  - periodically reviewed
- Entity exceptions documented, approved, and tracked
- Exceptions < 3%

Implementation

- Controls implemented consistently across the entity
- Evidence exists for all activities
- Metrics are captured and reported
- Target values for metrics are defined

- Exceptions < 5%

This maturity level requires local measurement, even if tools are group-owned

Level 5 – Optimizing

Documentation

- Group documentation continuously improved
- Entity feedback actively incorporated
- Exceptions < 0.5%

Implementation

- Continuous improvement demonstrable
- Metrics show consistent improvement over time
- Exceptions < 1%
- Lessons learned systematically drive updates

This maturity level would only be achievable if entities actively contribute, not just passively consume group controls

Avoiding a common scoring mistake

Incorrect interpretation

The entity does not have its own policy ➔ documentation maturity is Level 1

Correct CyFun interpretation

The entity formally adopts a group policy ➔ documentation maturity depends on approval, applicability, review and exception handling.

This distinction is crucial for group-based organisations.

General principle

Regardless of where CyFun® 2025 controls are defined or operated, the entity remains responsible for demonstrating that applicable controls are implemented and effective within its own scope.