OUTLIERS INTERNAL CONTROL CENTRE™

IT Controls Toolkit™

Control the IT environment (ITGC & cyber)

IT / IT Security / Internal Audit · Flagship Edition 2026

Outliers Professionals Ltd — Internal Control Centre Resource Library

1. Executive Overview

This toolkit controls the IT environment that underpins business systems — access, change, operations, backup and cyber controls, drawing on COBIT by name.

This toolkit is part of the Outliers Internal Control Centre™ and is anchored to COSO, the IIA Standards and the Three Lines Model (by name). It gives boards, management and assurance providers an applied, end-to-end kit to design, operate, test and report controls in this domain.

2. Objectives

The control objectives this toolkit helps you achieve:

- Control logical and privileged access
- Control system changes
- Operate and monitor IT operations
- Ensure backup and recoverability
- Operate cyber preventive and detective controls

3. Governance

IT controls are owned by IT (first line), overseen by IT risk/security (second line) and assured by internal audit:

Line	Role
Board / Audit Committee	Oversees the control environment and assurance
First line (management)	Owns and operates controls
Second line (risk/compliance)	Sets policy, monitors and supports
Third line (internal audit)	Provides independent assurance

4. Control Framework

The framework covers IT general controls — access management, change management, IT operations, backup and recovery — and cyber controls, drawing on COBIT governance and control principles (by name).

Maturity model

L1 Initial	L2 Developing	L3 Defined	L4 Managed	L5 Optimised
Informal / unreliable	Basic, inconsistent	Documented & standardised	Monitored & tested	Automated & value-creating

5. Roles & Responsibilities

Role	Responsibility
IT (1st line)	Operates ITGC and cyber controls
IT security (2nd line)	Sets policy; monitors access and security
Control owners	Perform access reviews and change approvals
Internal audit	Assures IT controls
Audit committee / Board	Oversees IT and cyber risk

6. Risk-Control Matrix (sample)

Illustrative risk-control matrix. The full working version ships as an editable XLSX with risk owner, control owner, frequency, type, design & operating effectiveness, status, due date and RAG.

Ref	Risk	Control Activity	Owner	Freq	Type
IT-01	Inappropriate	Provisioning &	IT Security	Quarterly	Preventive

	access	periodic access review			
IT-03	Unauthorised changes	Change approval and testing process	IT	Event	Preventive
IT-05	Data loss	Backups performed and recovery tested	IT Operations	Monthly	Corrective
IT-06	Cyber compromise	Logical security and monitoring	IT Security	Continuous	Preventive

7. Sample Controls

- User access provisioning and periodic review
- Privileged-access restriction and logging
- Change approval, testing and migration controls
- Batch/job monitoring and incident management
- Backup and tested recovery
- Logical security and security monitoring

8. Control Testing Approach

Test design first (is the control capable of mitigating the risk?), then operating effectiveness (did it operate over the period?). Use the assessment scale: Effective / Partially effective / Ineffective.

Control	Test procedure	Sample basis	Frequency
Access controls	Review access provisioning/removal for a sample	Sample	Quarterly
Change controls	Inspect change approvals and testing for a sample	Sample	Quarterly
Backup/recovery	Review backup logs and recovery test results	Sample	Monthly

Record results in the Control Testing Workpaper and log gaps in the Control Deficiency Tracker (both ship as editable files).

9. Implementation Roadmap

Phase	Focus	Outcome
Phase 1	Document IT landscape and risks	ITGC control map
Phase 2	Implement access and change controls	Operating ITGC
Phase 3	Add backup, operations and cyber controls	Controlled IT environment
Phase 4	Monitor and test	Assured IT controls

10. Templates

This toolkit is supported by the following editable templates and working files in the Resource Library:

- ITGC Control Matrix (XLSX)
- Access Management SOP
- Change Management Control SOP
- User Access Review Template
- Cyber Controls Checklist

11. Checklists

☐ Access management controls operating

☐ Privileged access restricted and logged

☐ Periodic user-access reviews performed

☐ Change management process enforced

☐ IT operations monitored

☐ Backups performed and recovery tested

☐ Cyber controls operating

☐ ITGC deficiencies tracked

12. Board Reporting Examples

Standard control report: executive summary · control effectiveness (RAG) · key metrics · deficiencies & remediation · decisions sought.

Metric	Current	Target	RAG	Action
Access reviews on time	90%	100%	Amber	Complete reviews
Change compliance	93%	≥95%	Amber	Enforce process
Backup success	97%	≥99%	Amber	Investigate failures
Privileged logging	Partial	Full	Red	Enable everywhere

13. Audit Committee Reporting

Illustrative one-page summary for the audit committee (replace with live data):

Item	Status	Commentary
IT general controls	Amber	Operating; access reviews completing
Change management	Amber	Compliance improving
Cyber	Amber	Monitoring maturing
Decisions sought	—	Approve privileged-logging rollout

14. RAG Examples

How to read the RAG status used across this toolkit and its workbooks:

RAG	Meaning	Control interpretation	Action
Green	Effective	Design and operating effectiveness both effective	Maintain and monitor
Amber	Partially effective	Design or operating effectiveness only partially effective	Improve and re-test
Red	Ineffective	Design or operating effectiveness ineffective; or critical deficiency	Escalate and remediate

Notes & Disclaimer

This resource is a professional internal-control template, not assurance, audit, legal or regulatory advice. It is anchored to COSO, COSO ERM, the IIA Standards, the Three Lines Model, ISO 31000, ISO 37301, ISO 9001 and COBIT, and to FRCN, NCCG 2018, SEC, CBN and NAICOM requirements — referenced by name only, with no copyrighted framework content reproduced. Calibrate control objectives, controls, owners, frequencies and thresholds to your organisation and confirm requirements against the current standards and applicable regulation. Bracketed fields [like this] and sample entries are editable, illustrative placeholders.