

Enhance your IT Audit and Risk Credentials

Auditing General Information Technology Controls (GITCs)

Topics today

- The role of internal auditors in GITCs
- Purpose of GITCs
- Scope of GITC review

IIA practice guides- Global Technology Audit Guides (GTAG)



Practice Guides — GAIT

Guide to the Assessment of IT Risk (GAIT)

The GAIT series of Practice Guides describes the relationships among business risk, key controls within business processes, automated controls and other critical IT functionality, and key controls within IT general controls. Each guide addresses a specific aspect of IT risk and control assessment.

Title	Date
GAIT Methodology	January 2009
GAIT for IT General Control Deficiency Assessment	January 2009
GAIT for Business and IT Risk	January 2009

Practice Guides — GTAG®

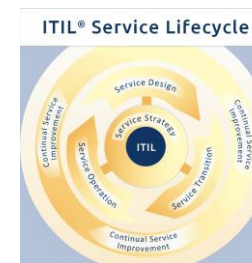
Global Technology Audit Guide (GTAG)

GTAGs are written in straightforward business language and address timely issues related to information technology (IT) management, control, and security.

Title
Assessing Cybersecurity Risk: Roles of the Three Lines of Defense
Auditing Application Controls (Previously GTAG 8)
NEW! Auditing Insider Threat Programs
Auditing IT Governance (Previously GTAG 17)
Auditing IT Projects (Previously GTAG 12)
Auditing Smart Devices: An Internal Auditor's Guide to Understanding and Auditing Smart Devices
Auditing User-developed Applications (Previously GTAG 14)
Business Continuity Management (Previously GTAG 10)
Change and Patch Management Controls: Critical for Organizational Success, 2nd Edition (Previously GTAG 2)
Continuous Auditing: Coordinating Continuous Auditing and Monitoring to Provide Continuous Assurance, 2nd Edition (Previously GTAG 3)
Data Analysis Technologies (Previously GTAG 16)
Developing the IT Audit Plan (Previously GTAG 11)
Fraud Prevention and Detection in an Automated World (Previously GTAG 13)
Identity and Access Management (Previously GTAG 9)
Information Technology Outsourcing, 2nd Edition (Previously GTAG 7)
Information Technology Risk and Controls, 2nd Edition (Previously GTAG 1)
Management of IT Auditing, 2nd Edition (Previously GTAG 4)
Understanding and Auditing Big Data

Role of Internal Auditors in GITCs

- Knowledge
- Investing in your knowledge
- Consultant or Assurance
- Independent Risk Assessments
- Design of controls
- Education
- Control Testing
- Application reviews



PRINCE2



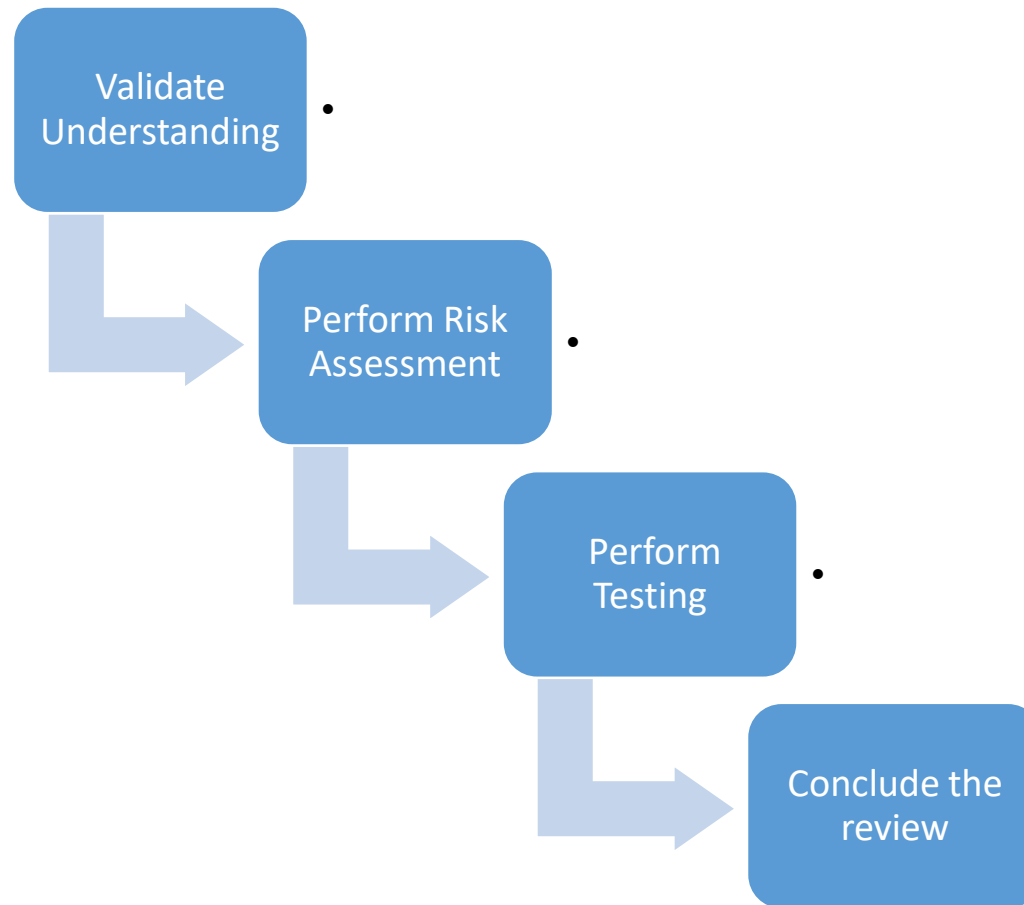
Why test GITCs?

- The dependency we have on IT systems
- Reliance on application controls
- Understand how the systems work
- Included in several operational and regulatory audits:
 - IT operational reviews
 - SOC-2 assessments
 - Payment Card Industry Data Security Standard (PCI DSS) reviews/audits
 - SOX-assessments
 - Project review assessments

Coverage of GITC

Application System	Access Security	System Change Control	Data Centre and network operations
Databases			
Operating Systems			
Network			

Risk-based Audit Approach



Validate Understanding

- Application
- Owner/Support
- Description
- Users
- Database
- Operating System
- Hardware
- Remote capabilities
- Products/services offered via the internet
- Previously identified issues
- Outsourced systems/processes

System Processes

- Transactions
- Batch processing
- Interfaces between systems

Access Security

- User access provisioning
- Generic Access and Privilege Access
- User access de-provisioning
- User access review
- Password parameters

Common Weaknesses

- User access de-provisioning
- Excessive access for some systems
- Weak password settings

System change control

- Change management policy
- Testing in development environment
- User Acceptance Testing
- Apply changes in production environment
- Segregation of duties

Common Weaknesses

- Segregation of duties
- No audit trail

Data centre and network operations

- Regular back-up
- Business Continuity Plan (BCP)
- Firewalls in place
- System updates or patch installations

Common Weaknesses

- BCP is not tested
- Patches not updated

Outsourced providers for infrastructure services

- Service level agreements
- Reporting
- Confirmation of control effectiveness

Common Weaknesses

- No control effectiveness review
- Unclear relationship management

Concluding on identified weaknesses

- Errors identified
- Mitigating controls
- Recommendations

Any Questions?

