IT General Controls

ACCA UK's Internal Audit Network held a series of seven webinars on de-mystifying IT audit for business auditors in 2017. The series started in May and concluded in November with a webinar about the General Data Protection Regulation (GDPR). It featured three main presenters - Vincent Mulligan FCCA (IT Audit Consultant at Eisteoir Consulting Ltd), Mike Hughes CISA, SGEIT, CRISC and Steve Connors CISM, FIPA, FFA (both partners at Haines Watts). To register to watch any of the webinars in this completed series, click here.

This article provides a few brief highlights of the second webinar in the series on IT general controls. In this session, the speakers considered the nature of ITGC, the challenges internal auditors face reviewing them and the approaches that you can use to audit them.

What are IT General Controls?

IT General Controls (ITGC) or General Computer Controls (GCC) are controls which relate to the environment that supports IT Applications. The appropriateness and effectiveness of ITGC's therefore impacts on all the organisation's IT applications.

IT general controls are policies and procedures that:

- Support application controls and IT components of manual controls
- Have a pervasive impact on controls at the application level
- Can relate to multiple applications
- Operate centrally or in multiple locations
- Support automated controls within applications

There are four main groupings of ITGC:

- Access to programs and data
- Program change
- Program development
- Computer operations

Why are ITGC important?

Organisations are increasingly dependent on IT and have increasingly complex operational and financial IT systems. IT General Controls have an impact on the controls over all financial IT systems:

  - Effectiveness and efficiency of information management
  - Reliability of information assets
  - Compliance with applicable legal, regulatory and business requirements
  - IT controls can have implications over manual as well as automated controls.

"Auditors cannot rely on automated controls if ITGC are not effective – if the foundations are not there then you cannot rely on what you have built upon those foundations."

When should we audit IT General Controls?

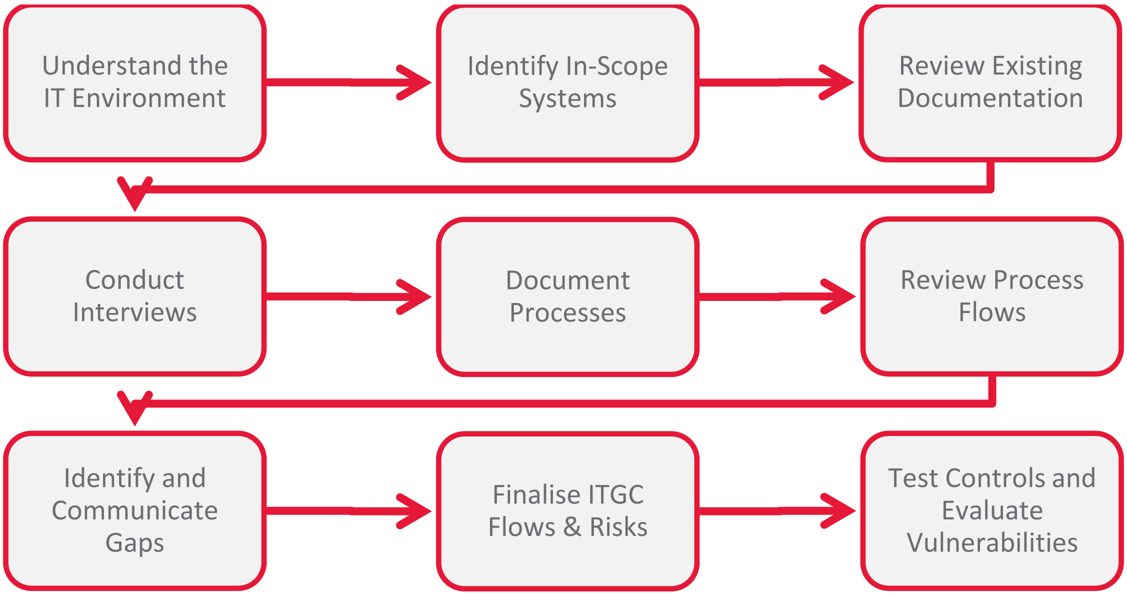
Any weakness in IT general controls will have an impact on the application controls audit so it is important that you look at IT general controls at an early stage so that you can wrap that into your planning of application audits. Timing will also be influenced by annual audit planning, changes in the IT environment, and events and emerging risks.

You will need to consider what skills and experience is required to effectively audit ITGC the timing of work (before or after implementation of any IT projects), and specific risks to your environment.

How do we audit IT General Controls?

When auditing IT General Controls, you can audit them as separate control audits or you can incorporate some IT General Controls work into IT functional audits. Integrated audits can build on work that has already been done in relation to general computer controls. However we are not just relying on auditors – these are controlled environments so there are other business assurance processes such as continuous monitoring, vendor audits, etc which will also provide assurance. When you are thinking about getting assurance over IT General Controls, in addition to audits you should consider the other mechanisms we use to get assurance – such as taking part or observe at steering committees, and also ensuring you have access to metrics and dash boards that will give you a view as to what is currently happening in the IT environment. This can inform your view on the annual planning process and what they may need to change.

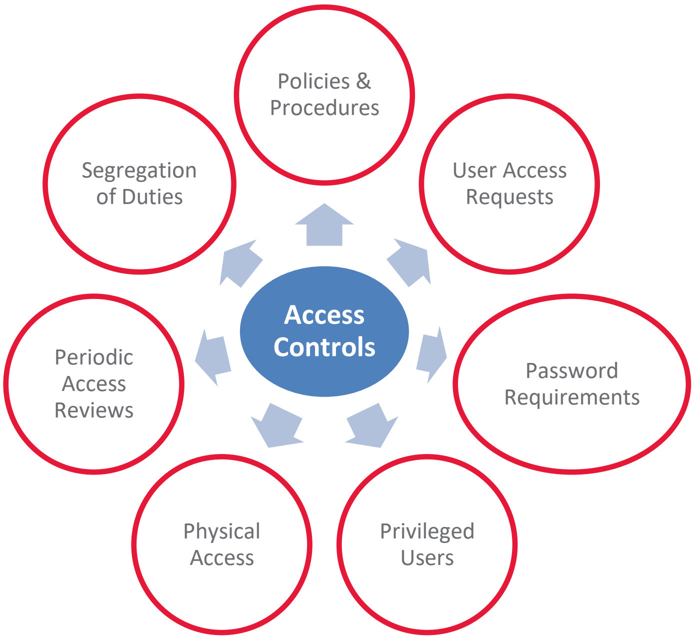
A standardised vision of what an IT General Controls audit looks like this:


Understand the IT Environment
Identify In-Scope Systems
Review Existing Documentation
Conduct Interviews
Document Processes
Review Process Flows
Identify and Communicate Gaps
Finalise ITGC Flows & Risks
Test Controls and Evaluate Vulnerabilities

Access to Programs and Data

The risk is that unauthorised access to data may result in the destruction or change of data, either malicious or accidental. This could include the recording of inaccurate or fraudulent transaction. The objective is to implement access controls to restrict access to specific programs and data to only those who are authorised to do so.

When we are auditing access controls, we are not talking about one process – we are talking about multiple processes that layered together give us the layers of defence that create the secure environment. Some of the layers that we would expect to see in an IT General Controls framework:



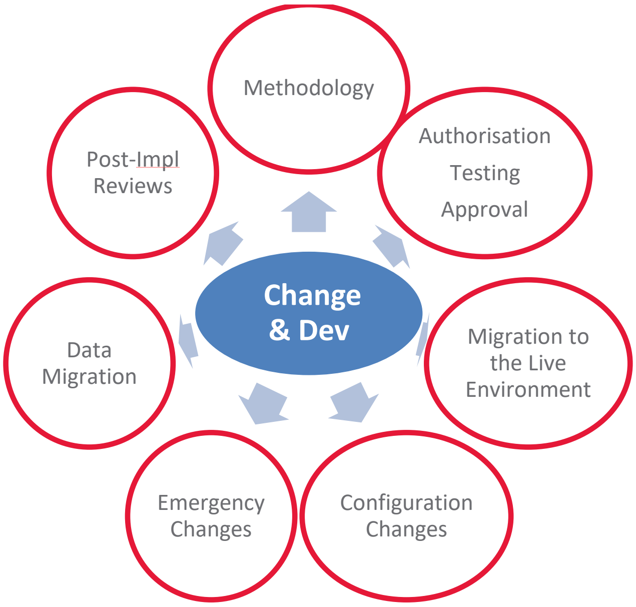
A walkthrough of IT General Controls provides the opportunity to understand what controls are in place and how they are operating. With testing, we want to know what actual access has been granted - we know what the system owner has approved because we have seen that during the walkthrough but now we want to validate what is actually happening. Without testing, we cannot get the level of assurance that we want that the controls are working and that there aren't any weaknesses or failures to implement the policies throughout the period. Examples of walkthrough and testing are summarised in this table:

Walkthrough	Testing
• Logical access controls at the operating system/database level • Security logs/review • Process for starters/leavers/changes • Periodic review of user access • How is SoD achieved – consider access to development, testing and live environments as well as multiple user accounts • Environmental controls – visit data centre/server room • What is the process for setting up/terminating access to the server room/data centre	• Existence of security policy and communication Sample of users – incl password resets, matching of access to job role, super user, review of violation logs • Sample of starters/leavers/changes – appropriately authorised and timely • Periodic review of user access – evidence • Sample of users with access to development/test/live – consider appropriateness of SoD, evidence of conflict • Evidence of testing environmental controls • Data centre access: • Compare to staff list • Test to ensure unauthorised users can't access

Program Change and Development

This relates to the development of applications and after they have been running live for some time, how changes are made. The risk is that unauthorised amendments to systems or programs may result in attacks (eg. denial of service) or fraudulent activities. The objective is to have robust program change management controls to ensure all changes to systems and applications are authorised, tested, documented and approved. Further, programme development should follow a similar system of authorisation, testing, approval and implementation.

Key areas to be considered in change and development audits:



Walkthrough and testing for program changes:

Walkthrough

End to end processing of a change request

- Consider planned/unplanned and emergency changes
- Logging of request
- Testing
- Move to production ('live') environment
- Documentation update
- Change scheduling
- How would an unauthorised change be identified

Testing

Existence of change procedures

- Sample of change requests:
  - Approval
  - Testing/UAT/sign-off
  - Retention of documents (e.g. testing requests/sign off)
  - Existence of separate environments for testing/QA/staging
  - Documentation update
- Review of change logs against change requests
- Users who can promote changes to live

Walkthrough and testing for program development:

Walkthrough

End to end processing of a development project

Development lifecycle

Project management

Procurement of IT equipment (software/hardware/infrastructure)

Implementation of the project

Testing

Existence of systems development lifecycle

Sample of developments:

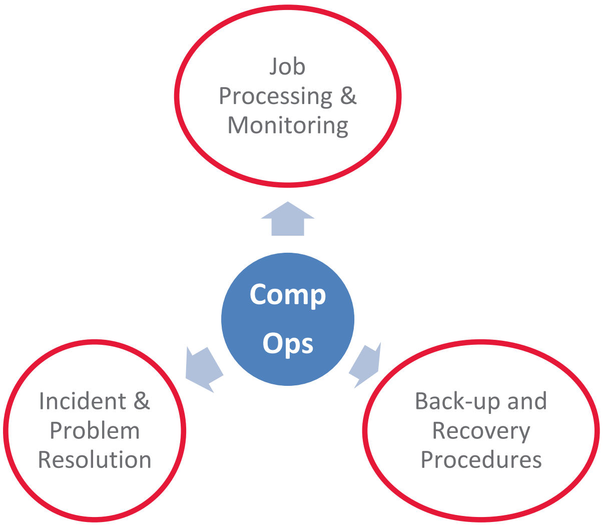
- Confirm to development lifecycle/methodology
- Appropriate approvals
- Testing/UAT/sign-offs
- Migration process – including data migration
- Testing of interfaces
- Document retention
- Training
- Documentation is produced/updated
- Governance (risk assessment/reporting/management)
- Post go live review

Computer operations

This is fundamentally about service management and service delivery – is the service that is being provided what the business requires. For example, IT support hours should mirror business requirements. Another example is whether patch management is up to date to prevent malware attacks.

The risk is that systems and applications are inaccurately processing data and/or processing inaccurate data. The objective is to have controls to ensure that system and application processing operations are authorised, and any deviations from normal behaviour are identified, investigated and ultimately resolved.

Key areas to be considered:



Comp Ops

Job Processing & Monitoring

Incident & Problem Resolution

Back-up and Recovery Procedures

Walkthrough and testing for computer operations:

Walkthrough

- Backup and recovery procedures
- Periodic testing – file recovery/restore
- Back up storage
- End to end process for incident management (incl escalation)
- Incident/problem tracking – helpdesk facilities and software
- Monitoring of live environment to identify failures
- Job processing – including how exceptions are actioned (e.g. if an interface fails to load)

Testing

- Sample of backup logs to ensure no exceptions/errors.
- Sample of failed backups – what action was taken?
- Evidence of recovery testing and results of last test
- Sample of requests for file restores
- Physical & environmental controls over access to and storage of back up tapes etc. or going forward, the cloud
- Sample of incidents/failures – confirm acted upon appropriately
- Sample of job processes to ensure completed
- Sample of scheduling failures to ensure appropriate action taken

These have been very brief highlights of the webinar - to register to watch the whole webinar, and any of the other webinars in this completed series, click here.