Internal Controls over Financial Reporting

Integrating in Business Processes & Key Lessons learned
Stephen McIntyre, CA, CPA (Illinois)

Senior Manager at Ernst & Young in the Risk Advisory practice.

Worked in the Assurance/Audit practice for 9 years performing financial statement auditing on industry and government clients (small to large).

Agenda

► Internal Controls over Financial Reporting
  ► Entity Level
  ► Transaction Level
  ► IT General Controls

► Key lessons learned

► Q&A
Evolution of ICFR

SOX 404  NI 52-019  PIC
Internal Controls Over Financial Reporting (ICFR)

- Internal control is a well defined term. The true value and basis of evaluation of internal controls is generally not well understood..

- Internal control evaluation = behavioural evaluation

- Internal controls provide a means of efficiently testing sample pieces of data in order to conclude on the entire population.
Benefits of ICFR

ICFR can provide the reader of financial statements with:

- Assurance that financial statements fairly reflect all financial transactions;
- Assurance that all transactions are recorded in accordance with applicable policies, directives and standards;
- Assurance that transactions are carried out in accordance with delegated authorities;
- Assurance that financial resources are safeguarded against material loss due to waste, abuse, mismanagement, errors, fraud, omissions and other irregularities;
Benefits of ICFR

► Providing assurance (audit level 95%) is much easier when you can assess the consistency with which transactions/events are processed.

► Auditing on a purely substantive basis is costly, and not auditing at all can be even more so in the long run.

► Assessing the effectiveness of internal controls provides the starting point to providing any level of assurance.
Key concepts / definitions

► **Design effectiveness**: The right person, using the right information to make the right decision in a timely manner, to mitigate identified key risks.

► **Operational effectiveness**: The consistent application, without exception, of an effectively designed control.
Key Components of ICFR
Top down, risk-based approach

The overall objective of an effective system of internal controls over financial reporting is to provide an effective and efficient means of auditing the financial results.

Equally important is the efficiency and effectiveness of the internal control and risk identification strategy.

One of the most common pitfalls is the over identification of risks related to the organization’s financial reporting.

Using a top down, risk-based approach will address the requirements of ICFR while maintaining efficiency throughout the organization.
Internal Controls over Financial Reporting

Entity Level Controls

Transaction Level Controls

IT General Controls
Top down, risk-based approach

Entity Level Controls

► Using the COSO framework as a guide, the control environment plays a significant role in the overall internal control system.

► Entity level controls (ELC), provide the “tone at the top” of the organization, and as a result directly or in-directly impact all underlying controls.

► Effective ELC’s can provide excellent leverage to reduce testing at lower levels. Ineffective ELC’s can spell disaster for all underlying controls.

► ELC’s exist in two forms, direct and indirect.
Top down, risk-based approach
Entity Level Controls

► Direct entity level controls monitor specific business and financial risks, and operate at the level of precision necessary to detect breakdowns in the application of an organization’s policies and procedures.

Example: CFO and Director of Finance review the quarterly and annual financial statement and related disclosures.

► Indirect entity level controls help define the control consciousness of an organization without directly mitigating any one specific financial or operational risk.

Example: An organizational code of conduct distributed via the intranet
Top down, risk-based approach
Entity Level Controls

1. The risk assessment identifies high, moderate and low risk areas

2. ELC’s may mitigate selective risks directly, reducing the need for detailed transaction level testing

3. What remains are higher risk areas that require more attention
Top down, risk-based approach
Entity Level Controls

- Benefits from leveraging effective ELC’s:
  - Reduce the extent of reliance on transaction level controls
  - Increase the effectiveness of internal controls through leveraging senior and experienced personnel
  - Better define and communicate the expectations of management across the organization (i.e., tone at the top)
  - Reduce redundancy in controls performed across the organization at different levels
Top down, risk-based approach
Entity Level Controls
Internal Controls over Financial Reporting

Entity Level Controls

Transaction Level Controls

IT General Controls
Top down, risk-based approach
Design of transaction level controls

► The starting point for assessing the effectiveness of the transaction level controls is defining what business processes are in scope.

► In order to assess the ICFR, you need to work backwards from the end objective, which in this case is the financial statements.

► Step 1 – identify the significant accounts
► Step 2 – associate the significant business processes
► Step 3 – perform a detailed risk assessment
Top down, risk-based approach

Design of transaction level controls – Sig. Accounts

- Determination of what accounts are deemed to be “significant” is a matter of judgement.

- Assess the materiality of the underlying account results, and assess the inherent risks related to each account

- A combined risk based approach uses the results of these two approaches to determine significance of each account presented on the financial statements.
Top down, risk-based approach
Design of transaction level controls – Sig. Accounts

► Each financial statement account is comprised of financial statement assertions:
  ► Existence / Occurrence
  ► Completeness
  ► Valuation
  ► Presentation & Disclosure
  ► Rights & Obligations

► From a risk based perspective, each assertion by significant account must be considered to prioritize the extent of identified risks.

► Example: Generally speaking, the risk of completeness is greater for liability based accounts than asset accounts.
Top down, risk-based approach
Design of transaction level controls – Sig. Processes

► The value associated to each significant account is derived by a specific set of business process(es). Don’t forget disclosure!

► A significant process can be associated to one specific account or several accounts across the financial statements.

► In order to effectively and efficiently perform the risk assessment, you must consider each business process and related transaction processing from initiation to recording.

► Example: Procurement of a good or service is most commonly initiated through requisition completed by the end user. If during the scoping exercise an organization was focused purely on the traditional “accounting” functions, key risks could be over looked.
The key objective in risk identification is to focus on key risks related to financial reporting (and disclosure).

Without appropriate identification of the significant accounts, related assertions and processes, the risk identification process can easily go beyond the applicable scope of ICFR.

Ask the question “What could go wrong” specific to the account/assertion/process.

**Hint:** A key risk, if not mitigated by a control (or suite of controls), could cause a material error to the financial statements.
Top down, risk-based approach

Design of transaction level controls - Controls

► Focus on identifying the key controls related to the identified key risks.

► Each identified key risk must have at least one associated key control.

► Where one key control is associated to several key risks, and is the only key control associated to those risks, the greater the risk that control failure could result in a material error and therefore the greater reliance being placed on this “super control”.

► Controls can be preventative or detective in nature. Ideally, a mix of both should be identified.
Internal Controls over Financial Reporting

Entity Level Controls

Transaction Level Controls  IT General Controls

Quality in Everything We Do
The Importance of ITGCs

- IT controls protect data integrity and are a significant component of an organization’s ICFR.

- IT controls relate to the security (confidentiality, integrity, and availability) of data, as well as the overall management of the organization business functions.

- Information systems support the flow of information from initiation to recording and are one of the most important and pervasive pieces of an organization’s financial reporting system.

- IT systems are increasingly relied upon as tools to provide efficient processing and reporting for decision making purposes.
The Importance of ITGCs

- Reduce the extent of testing and reliance on manual transaction-level controls

- Increase the effectiveness, efficiency and reduce costs of internal controls by establishing a sound information system foundation and leveraging systems across the organization

- Improve the consistency of control operation (i.e. automated processes vs. manual)

- Improve the security (confidentiality, integrity and availability) of corporate information

- Improve reliability of manual controls dependent on IT information
Operational Effectiveness

► The goal is to evaluate the consistency of control operation.

► Controls are tested based on the frequency of performance (daily, weekly, monthly, quarterly, annually)

► Test samples are not selected based on materiality

► Can/should exceptions exist?
Key Lessons Learned
As noted earlier the key to designing effective internal controls is understanding and defining the expected pattern of behaviour.

**Understanding the purpose of the control:** It’s important that the process owners understand why they’re performing the control and not just completing b/c they’ve been told to.

**Responsibility for the control:** Where process owners are selected without direct ownership of the process or related control, the likelihood of receiving timely updates is drastically reduced.

**Consistency is critical:** In order to rely on a pattern of behaviour (performing the control) as a predictor of an outcome (transaction processing), the behaviour must be performed consistently without exception.
Lessons Learned – Control design

► **Defining the expectation for operation:** Starting to test a controls operation before you’ve defined what the expected output (evidence) of that operation will be is counter productive.

► **Documentation of your work:** SOX 404 requires an independent assessment, NI 52-109 and PIC are management only conclusions. However, unsupported assertions would in and of themselves be evidence of weak governance.

► **Rotational design assessments:** Rotational based assessments can provide a level of efficiency, however the basis upon which you chose to leverage this model must be validated every year.

► **The right number of key controls:** There’s no magic number when it comes to key controls, however not every risk is a key risk, equally not every control is a key control.
Lessons Learned – Control design

► **Performing controls differently across an organization**: This is an issue for large organizations with decentralized structures. Allowing multiple processes allows flexibility across regions, however increases the risk of inconsistent application.

► **Heavy reliance on detect controls**: Effectively design internal control structures include both prevent and detect type controls. Relying too heavily on either type can produce additional risks for control failure.

► **Involving other groups in the organization**: When identifying key risks and related controls, areas outside of finance/accounting can have direct/indirect impacts on financial reporting. Getting process owners from these groups on board early in the project can be critical to future success (IT, HR, Legal etc).
Lessons Learned – Control operation

► **Reporting Findings and weaknesses** – When a control has failed, the key question is whether it failed b/c of poor design or poor operation. Not understanding why a control did not operate as expected can lead to continued failures in the future.

► **Impact of control failure** – When reporting findings it’s important to assess the residual risk of a control failure. If control x fails, what are the direct impacts? Do we have mitigating controls? Have we evaluated those mitigating controls? Being prepared for these questions when presenting to senior management is key.

► **Errors in Financial Reporting** - Control failures increase the risk of reporting errors, identified reporting errors commonly signal control failures. Materiality isn’t the real issue...
Lessons Learned – Control operation

► Remediation Plans – Control failures occurred, how will they be remediated? Creating an action plan to correct control failures requires (1) understanding the nature of the failure, (2) understanding the risk presented by the control not operating as designed, (3) understanding mitigating controls.

► Relying on other organizations – Organizations increasingly rely upon outside service providers who directly or indirectly impact financial reporting. Gaining comfort over what that service provider is doing can vary:
  ► Industry – organizations complying with SOX and NI52-109 are required to obtain sufficient assurance from the service provider through substantive means (service auditor reports) and/or identify controls which mitigate the risk caused by the participation of a third party (i.e. review of assumptions used in complex calculations).

  ► Federal Government – under the PIC, department’s receiving 3rd party services from other govt departments can rely on that parties PIC statement.
Common ITGC points of failure…

► We have over 100 systems and applications, I don’t have time for this...
  ► The nature of ITGCs are such that they fall both within the realm of the IT department as well as the operational/functional departments who rely upon them. As a result, there is a lack of ownership for documenting and understanding them.
  ► As with any other type of control, proper scoping of the key systems and applications is critical. Often the IT inventory can be confusing and leads to too many or not enough assessment being performed.

► We’ve been audited for “x” years, the controls have already been tested and firm “y” relies on them...
  ► Unless the auditor has specifically noted his/her opinion to include an assessment of internal controls, you can’t make that assumption.
  ► SOX 404 remains the only requirement for an independent assessment of control effectiveness, and its issued separately from the audit opinion.
Common ITGC points of failure...

► Everyone updates their passwords regularly...
  ► There is more to logical access than passwords, however it is surprising how many times this simple control is overlooked or assumed to be operating effectively.
  ► Password changes are done too infrequently.
  ► Passwords are written down on post it notes and placed beside the computer.

► We’re a small organization, we’ll know when someone has left....
  ► When employees leave their access to systems, networks, applications must be turned off. Failures in processing these changes typically stem from (1) lack of communication (HR to IT), or (2) lack of understanding around risks (i.e. Only network access removed)

► Our IT group is very small, there’s no need for an assessment...
  ► Risks exist for small and large IT groups, how they differ is important in considering the design effectiveness.
Lessons learned

► **User termination** – Departures should be timely
  - Terminating user access to applications, databases, operating systems and networks is challenging, as it’s not a function owned by only one group within the organization (for instance, Human Resources, Finance, IT)
  - Similarly, when an employee changes positions within the organization, their access requirements also change and require timely modification

► **Segregation of duties** – Development and production environments:
  - Preventing developers from accessing the production environment for key IT systems can be a challenge,
  - Particularly for small organizations where the number of IT resources is limited
  - Practical solutions will allow key individuals to continue providing services (i.e. IT support), while still maintaining data integrity, which is key
Lessons learned

► More than an IT issue - IT general controls, are NOT sole responsibility of IT:
  ► Numerous key IT control activities require responsibilities of business representatives
  ► For example: Approving application-level access rights
  ► All IT stakeholders, inside and outside of the IT branch, should be actively involved in ICFR projects

► Process consistency – Project efficiency achieved through consistent ITGCs:
  ► Achieve consistency across an organization’s systems (activities pertaining to multiple systems within an organization are consistent; for example, the process of terminating access to a system when employees depart the organization)
  ► Streamline IT general control testing
  ► Maintain operating effectiveness of IT general controls on an on-going basis by reducing the degree of variance in manual activities across the organization

► IT control selectivity—Carefully consider systems and controls in scope:
  ► Give priority to core applications directly impact financial reporting
  ► Identify risks specific to that objective
  ► Avoid starting with too broad a scope, which can result in lost efficiencies
Questions & Answers