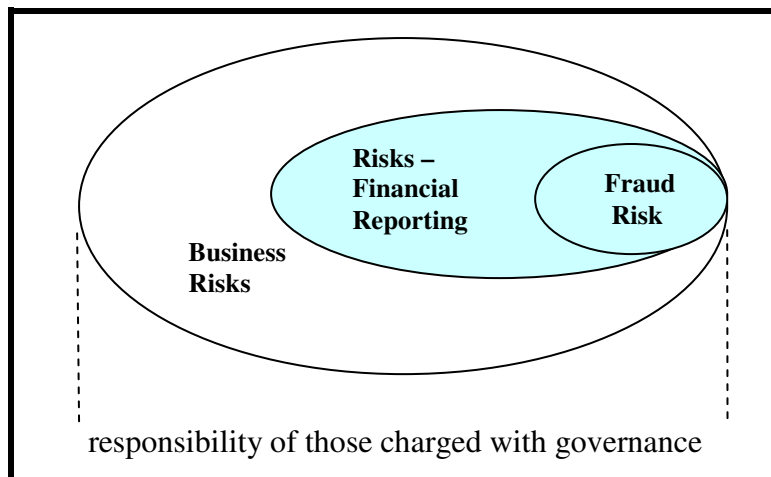


information on RISKS, from the auditor's perspective of *professional scepticism*

risk examples

- it is possible that account balances, classes of transactions or financial report disclosures may be incomplete, inaccurately stated or missing altogether from the financial report. Examples might include:-
 - understated liabilities
 - unrecorded assets
 - assets such as cash/equipment that may have been misappropriated and
 - missing/incomplete disclosures
- areas of vulnerability where *management override* and manipulation of the financial report could take place. Examples could include:-
 - preparation of journal entries
 - revenue recognition policies
 - management estimates
- other control weaknesses that, if not corrected, could lead to material misstatements in the financial report.

risk categories



limitations of a risk-based audit

limitations	reasons
use of testing	Any sample of less than 100% of a population introduces some risk that a misstatement will not be detected.
internal control limitations	Even the best designed and most effective controls can be overridden or negated by management, or by collusion among employees.
fraud that goes undetected	Because fraud is specifically designed not to be detected, there is always the possibility that it will not be discovered.
nature of audit evidence available	Most audit evidence tends to be persuasive in character rather than conclusive.
availability of audit evidence	Insufficient support may be available for drawing absolute conclusions on specific assertions such as fair value estimates.
reliance on judgments made by the auditor	Professional judgment is required to:- <ul style="list-style-type: none"> – appropriately identify and address risk factors – decide what evidence to gather – assess estimates made by management and – draw conclusions based on the evidence and management representations.
difficulty in ensuring completeness	There is a risk that some important information is not known about, not obtained or has been concealed from the auditor.

risks associated with IT internal controls

- reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both
- unauthorised access to data that may result in destruction of data or improper changes to data, including the recording of unauthorised or non-existent transactions, or inaccurate recording of transactions (particular risks may arise where multiple users access a common database)
- the possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties, thereby breaking down segregation of duties
- unauthorised and/or undocumented changes to data in master files
- unauthorised and/or undocumented changes to systems or programs
- failure to make necessary changes to systems or programs
- inappropriate manual intervention
- potential loss of data or inability to access data as required.

fraud and environment for fraud

The term “fraud” refers to an intentional act by one or more individuals among management, those charged with governance, employees or third parties, involving the use of deception to obtain an advantage.

Fraud involving one or more members of management or those charged with governance is referred to as “management fraud”. Fraud involving only employees of the entity is referred to as “employee fraud”. In either case, there may be collusion within the entity or with third parties outside the entity.

Some of the major conditions that create an *environment for fraud* include:-

- ineffective corporate governance
- lack of leadership and “tone at the top” by those charged with governance and management
- high incentives provided for financial performance
- complexity in entity rules, regulations, and policies
- unrealistic budget targets for staff to attain
- inadequate internal control, especially in the presence of organisational change.

As can be determined from the above, the most effective anti-fraud internal control would be a strong commitment by those charged with governance and senior management to doing the right thing. This is evidenced through articulated entity values and a day-to-day commitment to ethical behaviour.

anti-fraud controls

These are controls designed by management to prevent, detect and/or correct frauds. With respect to management override, these controls may not prevent a fraud from occurring but would act as a deterrent and make perpetrating a fraud more difficult to conceal. Typical examples are:-

- policies and procedures that provide additional accountability, such as signed approval for journal entries
- spot-checking by senior management and requiring employees to take their annual leave entitlement
- improved access controls for sensitive data and transactions
- silent alarms
- discrepancy and exception reports
- audit trails
- fraud contingency plans
- human resource procedures such as identifying/monitoring individuals with above-average fraud potential (e.g. indicated by a lavish lifestyle)
- enabling potential frauds to be reported anonymously.