The five components of internal control

MODULE 2 | 2.5.1 | STUDENT COMPANION

Internal control has **five components**: the control environment, the way the entity assesses risk, its process for monitoring the system, the information system and communication, and the control activities. The auditor must understand each one and evaluate the design of the controls that matter most. Every system has **limitations**, above all collusion and **management override**, and a small business relies on its owner, who is both its best control and its biggest risk.

What internal control is

Internal control is the process that the board, management and other staff design and run so the entity can be reasonably confident of meeting its goals for **reliable financial reporting**, **effective and efficient operations**, and **compliance with laws and regulations**. The auditor must understand each of the five components, evaluate the design of the controls that matter most to the audit, such as controls over significant risks and over journal entries, and check that they have actually been put in place. **Understanding isn't testing:** understanding asks whether a control is well designed and exists; testing (Module 3) asks whether it worked throughout the period.

The five components of internal control

	What it covers	At Voltana (imagined)
Control activities	The actions that make sure management's directions are carried out	See the next diagram
Information system and communication	How transactions are started, recorded, processed, corrected, posted and reported, with the IT behind them; how people learn their roles	An installer's completion form from a phone, revenue in the new system, a monthly report to the board
Monitoring the system of internal control	Ongoing checks such as monthly results against budget; separate evaluations such as internal audit; fixing deficiencies	A small internal audit team of two
The entity's risk assessment process	Identifying financial reporting risks, judging their significance and likelihood, and deciding how to respond	A clear process for currency risk, with foreign exchange contracts, but no formal assessment of the new system's risks
Control environment: the foundation	Integrity and ethics; oversight by an independent board and audit committee; management's style; authority and responsibility; hiring, training and accountability	A powerful founder-CEO with a large stake, and bonuses that reward revenue growth: does the board really challenge management?

Read from the bottom up: weaknesses in the foundation undermine everything above it

Five kinds of control activity

Authorisation and approval
A manager must approve any discount above 10%
Prevents

Reconciliation
The bank accounts are reconciled to the ledger every month, and each reconciliation is reviewed
Detects and corrects

Verification
The system matches each supplier invoice to the purchase order and the goods received record before payment
Prevents

Physical and logical controls
Stock in a locked warehouse, counted regularly; only authorised staff can change prices in the system
Prevents and detects

Segregation of duties
The person who sets up a new supplier can't also approve payments to that supplier
Prevents

Each is designed to stop an error or fraud happening, or to catch and fix it quickly

Why controls can't give absolute assurance

Human error
Mistakes in judgement, misunderstood instructions, tiredness

Collusion
Two or more people working together get around segregation of duties

Cost
Controls cost money, so some risks are accepted

Unusual transactions
Controls are designed for routine transactions, so unusual ones can slip past

Management override
For example, recording a journal entry that nobody else reviews

The limitation auditors worry about most: the people with the most power over the records are the ones the controls find hardest to stop

That's why internal control gives reasonable, not absolute, assurance

Case note: Westpac and AUSTRAC

In November 2019 AUSTRAC, Australia's financial intelligence agency, began proceedings alleging that Westpac had breached the anti-money laundering and counter-terrorism financing laws more than 23 million times. Most of the alleged breaches related to its failure to report more than 19.5 million international funds transfers, worth over $11 billion, over about five years. AUSTRAC also alleged failures to pass on information about the source of transfers, to assess and monitor the risks of its relationships with overseas banks, and to monitor accounts for patterns associated with child exploitation. The chief executive resigned that month, and in 2020 Westpac agreed to pay a penalty of $1.3 billion, approved by the Federal Court.

Source: AUSTRAC statement of claim and media release (November 2019); Federal Court of Australia penalty judgment (2020).

Through the five components: the information system didn't produce the reports the law required; risk assessment didn't properly assess a risky channel of business; monitoring didn't detect the gap for years; and the scale of the failure raised serious questions about the control environment. **For the auditor**, it means a liability for penalties to estimate and disclose, and non-compliance with laws to respond to.

Internal control in a small business

A small entity may have too few people to separate duties, and its controls are often informal. Its best control is often the owner-manager's own involvement: approving every payment, reading the bank statements and knowing the customers. But the same owner can override any control, so the auditor weighs the owner's integrity and usually relies more on substantive evidence. **Compensating controls** help, such as the owner reviewing a monthly list of new suppliers, or bank statements going straight to the owner unopened.

Practice questions

MODULE 2 | 2.5.1 | TRY THESE BEFORE THE WORKED ANSWERS

Question 1 - Which component?

Tillbrook Rural Supplies Ltd (imagined) sells seed, fencing and farm equipment through twelve branches. Say which of the five components of internal control each control belongs to.

Control	Component
(a) Every employee signs the code of conduct each year, and breaches lead to disciplinary action.	
(b) The audit committee, made up of independent directors, meets the external auditor each year without management present.	
(c) Each quarter, the finance team lists the risks to the accuracy of the financial reports, rates each by likelihood and impact, and assigns someone to respond.	
(d) Internal audit tests the purchasing controls at two branches each year and reports to the audit committee.	
(e) The chief financial officer compares monthly results with budget and follows up the causes of large differences.	
(f) A process map shows how a sales order moves from the online store into the general ledger and the monthly accounts.	
(g) A finance manual tells each branch manager what to report, to whom and by when.	
(h) Credit notes over $2,000 need the sales manager's approval.	
(i) Seed and fencing wire are kept in a locked store and counted every month.	
(j) Staff who raise purchase orders can't approve supplier invoices for payment.	

Question 2 - Find the weaknesses

Greenhaven Landscapes Pty Ltd (imagined) designs and builds gardens. The owner spends most days on job sites. When a supplier's invoice arrives by email, the office manager enters it into the accounting system and pays it through internet banking every Friday; the owner has given the office manager his internet banking token so payments aren't held up. The office manager also sets up new suppliers and changes their bank details whenever a supplier emails a request. Invoices aren't matched to orders or delivery dockets, because 'the crews know what they ordered'. The bank account is reconciled once a year, by the external accountant. Identify four control weaknesses and suggest a control activity for each.

Weakness	Control activity to fix it

Question 3 - Westpac through the five components

Using the five components of internal control, explain how the failures alleged at Westpac could happen in a large bank with thousands of controls.

Worked answers

MODULE 2 | 2.5.1 | WORKED ANSWERS - ATTEMPT THE QUESTIONS FIRST

Question 1 - Tillbrook Rural Supplies

	Component
(a)	Control environment: integrity and ethical values, enforced
(b)	Control environment: independent oversight by those charged with governance
(c)	The entity's risk assessment process
(d)	Monitoring the system of internal control: a separate evaluation
(e)	Monitoring the system of internal control: an ongoing check built into management's work
(f)	Information system and communication: how transactions flow to the ledger and the reports
(g)	Information system and communication: people learn their roles and what to pass on
(h)	Control activities: authorisation and approval
(i)	Control activities: physical controls, with a count as a check
(j)	Control activities: segregation of duties

Question 2 - Greenhaven Landscapes (any four)

Weakness	Control activity
One person sets up suppliers, enters invoices and pays them	Segregation of duties: someone else sets up and changes supplier records, or the owner approves every new supplier
The owner's banking token is used by the office manager, so nobody independent authorises payments	Authorisation: the owner keeps the token and releases each payment run after reviewing it; or the bank requires two approvals
Bank details are changed on the strength of an email	Verification: confirm every change by phoning the supplier on a number already on file, before any payment
Invoices aren't matched to orders or delivery dockets	Verification: match each invoice to an approved order and a signed delivery docket before paying
The bank account is reconciled only once a year	Reconciliation: reconcile monthly, with the owner reviewing and signing it; bank statements go straight to the owner

Question 3 - Westpac (sample answer)

- **Information system:** the systems didn't produce the reports the law required, so millions of international transfers went unreported, however many other controls were working.
- **Risk assessment:** the bank didn't properly assess the risks of a risky channel of business, including its relationships with overseas banks, so no controls were designed for those risks.
- **Monitoring:** reviews didn't detect the gap for years, so the failures kept growing.
- **Control environment:** a failure on this scale raises serious questions about oversight and about how much compliance mattered, and the chief executive resigned.
- **The point:** thousands of control activities can't make up for weak components around them. A system is only as strong as its environment, its risk assessment and its monitoring.