DegreeLive

Bachelor of Commerce (B2001) | Level 2 • Part B Major | Monash University

Accounting Information Systems

Course Code: ACC2400 • Module 3 Notes

Module 3: Internal Controls, Fraud Prevention, Cybersecurity & IT Governance

3.1 The AIS Threat Landscape, Occupational Fraud & Australian Governance Duties

Because an Accounting Information System centralises an enterprise's financial records, payment rails, and proprietary commercial data, it is continuously exposed to threats arising from natural disasters, software defects, human error, and deliberate fraud or cyberattack. Under Australian auditing standard **ASA 240 *The Auditor's Responsibilities Relating to Fraud in an Audit of a Financial Report***, accountants distinguish between *errors* (unintentional misstatements or omissions in financial data) and *fraud* (intentional acts by management, employees, or third parties involving deception to obtain an unjust or illegal advantage).

Taxonomy of Occupational Fraud and Cyber Threats

Occupational fraud within AIS environments clusters into two primary schemes defined by the Association of Certified Fraud Examiners (ACFE):

- **Asset Misappropriation:** Theft or misuse of organisational resources. Common AIS-enabled schemes include *skimming* (stealing cash before recording), *lapping* (concealing theft of customer remittances by applying subsequent customer payments to earlier accounts), *check/EFT kiting* (exploiting clearing float across multiple bank accounts), *ghost employees* (creating fictitious staff in HR/Payroll master files), and *shell-company billing* (submitting fabricated invoices through compromised supplier master records).
- **Fraudulent Financial Reporting:** Intentional distortion of financial statements by management to meet ASX earnings guidance, debt covenants, or executive bonus targets—typically executed via premature revenue recognition (channel stuffing, improper cut-off), capitalising operating expenses, or suppressing AASB 137 provisions.

Complementing internal occupational schemes are external cyber-enabled financial threats, notably **Business Email Compromise (BEC)**—where attackers spoof supplier emails or compromise CFO credentials to alter BSB and bank account numbers in the Supplier Master File—and **ransomware** encrypting ERP databases and backups.

Cressey's Fraud Triangle and the Fraud Diamond

Criminologist Donald Cressey established that occupational fraud generally requires three simultaneous conditions, known as the **Fraud Triangle**:

1. **Pressure (Incentive):** A perceived non-shareable financial need (personal debt, gambling losses) or corporate performance target (breaching a bank interest-coverage covenant).
2. **Opportunity:** The perceived ability to commit the act and conceal it without detection—almost always created by *weak internal controls*, excessive user privileges, or absent segregation of duties.
3. **Rationalisation:** A cognitive justification allowing perpetrators to preserve self-esteem ("I am only borrowing the funds," "the company owes me overtime").

Wolfe and Hermanson later extended this model into the **Fraud Diamond** by adding a fourth element: **Capability**—the technical skill, positional authority, and stress tolerance needed to exploit control loopholes in complex ERP environments. From an AIS design standpoint, while management cannot easily observe private personal pressures or rationalisations, it exercises direct control over *Opportunity* and *Capability* by enforcing least-privilege access, automated matching, and independent monitoring.

Australian Statutory Governance Obligations

Internal control failures carry severe statutory consequences for Australian directors and officers under the ***Corporations Act 2001 (Cth)***:

- **Section 180(1) — Care and Diligence:** Directors and officers must exercise their powers with the degree of care and diligence that a reasonable person would exercise—a duty Australian courts and ASIC explicitly interpret to include maintaining adequate cyber resilience and financial oversight.
- **Section 286 — Obligation to Keep Financial Records:** Companies must maintain accurate financial records for seven years; inadequate AIS access logs or unverified spreadsheets can constitute a strict-liability breach.
- **Section 295A — CEO and CFO Declaration:** For listed entities, the chief executive officer and chief financial officer must formally declare in writing to the board that the financial records have been properly maintained and that the declarations are founded on a sound system of risk management and internal control operating effectively.

AIS Fraud Scheme	System Mechanism Exploited	Primary Preventive Control	Detective CAAT Query
Accounts Receivable Lapping	Cashier steals Customer A's payment and covers it later with Customer B's remittance.	Lockbox / direct EFT bank feeds; strict SoD between cash custody and AR posting.	Compare bank deposit slip dates against AR posting timestamps and customer aging spikes.
Shell Company Billing	AP clerk creates a fictitious supplier matching an employee's BSB/account and approves invoices.	Segregate vendor master creation from AP entry; mandatory ABN Modulo-89 & Eftsure checks.	Cross-join `Supplier_Master.BSB_Acct` against `Employee_Master.BSB_Acct`.

DegreeLive

AIS Fraud Scheme	System Mechanism Exploited	Primary Preventive Control	Detective CAAT Query
Ghost Employee Payroll	Supervisor or payroll clerk retains a terminated worker or invents a non-existent TFN.	HR-only onboarding; require unique TFN and mandatory physical/MFA login verification.	Match `Payroll_Run` against badge/system-login logs and duplicate bank accounts.
Threshold-Splitting Fraud	Staff split a $1,400 purchase into three $466 claims to evade a $500 approval limit.	Cumulative daily/weekly spend limits per vendor and employee P-Card.	`GROUP BY Emp_ID, Vendor_ID, Tx_Date HAVING COUNT(*) > 1` near threshold.
BEC Vendor Bank Diversion	External attacker spoofs supplier email requesting urgent BSB update prior to EFT batch.	Out-of-band phone callback to pre-registered number plus dual MFA change approval.	Daily audit alert listing all `Supplier_Master` bank-detail edits within 14 days of payment.

3.2 Internal Control Frameworks: COSO and COBIT 2019

To design defensible controls rather than ad-hoc patches, Australian corporations adopt internationally recognised governance frameworks: the **COSO Internal Control — Integrated Framework (2013)** for enterprise-wide assurance and **COBIT 2019** for information and technology governance.

The COSO Internal Control — Integrated Framework

COSO defines internal control as a process, effected by an entity's board of directors, management, and other personnel, designed to provide *reasonable assurance* (never absolute assurance, due to collusion, management override, and cost-benefit constraints) regarding achievement of objectives across three categories: **Operations** (effectiveness and efficiency), **Reporting** (reliability and timeliness of financial and non-financial disclosures), and **Compliance** (adherence to laws such as ATO tax rules and AASB standards). These objectives are achieved through five integrated components comprising 17 underlying principles:

COSO Component	Core Purpose	Illustrative AIS Principles & Practices
1. Control Environment	Sets the ethical tone at the top and organisational accountability structure.	Code of conduct under APES 110/ASX Principles; independent Audit & Risk Committee; clear authority delegation.
2. Risk Assessment	Identifies and analyses threats to achieving objectives, including fraud risk.	Annual cyber/fraud risk register; materiality thresholds; evaluating ERP upgrade & cloud migration risks.
3. Control Activities	Policies and procedures ensuring management risk responses are executed.	Segregation of duties, three-way matching, MFA, automated input validation, physical asset locks.
4. Information & Communication	Captures and disseminates relevant, quality data internally and externally.	Standardised Chart of Accounts, documented BPMN procedures, confidential whistleblower hotlines (Corporations Act Pt 9.4AAA).
5. Monitoring Activities	Evaluates whether all five components remain present and functioning over time.	Continuous automated exception alerts, internal audit reviews, SOC 2 Type II cloud vendor evaluations.

Figure 3.1: COSO Integrated Internal Control Architecture & Three Objective Pillars



COBIT 2019 for IT Governance

While COSO addresses enterprise-wide internal control, ISACA's **COBIT 2019 (Control Objectives for Information and Related Technologies)** provides granular IT governance aligned to business goals. COBIT cleanly separates *Governance* (evaluated and directed by the board under the **EDM** — Evaluate, Direct, and Monitor domain) from *Management* across four operational domains: **APO** (Align, Plan, and Organise), **BAI** (Build, Acquire, and Implement), **DSS** (Deliver, Service, and Support), and **MEA** (Monitor, Evaluate, and Assess). For accounting auditors, COBIT maps IT controls directly to financial statement assertions—ensuring, for instance, that database change approvals (BAI06) protect completeness and accuracy in automated revenue postings.

3.3 Segregation of Duties (SoD) & Quantitative Risk Analysis

Control activities are classified by timing into three complementary layers: **Preventive controls** (which deter errors or fraud before occurrence, such as access passwords and credit limits), **Detective controls** (which uncover anomalies after occurrence, such as monthly bank reconciliations and exception logs), and **Corrective controls** (which remediate damage and restore operations, such as database backups and reversing journal entries).

Segregation of Duties (SoD) Matrix

The single most important preventive control in accounting systems is **Segregation of Duties (SoD)**, which ensures that no single individual can both perpetrate and conceal a fraud in the ordinary course of duties. Specifically, three incompatible functional roles must reside with distinct personnel or independent system accounts:

1. **Authorisation:** Approving transactions, master-file changes (new suppliers, credit limits), or pay rate adjustments.
2. **Custody:** Handling physical cash, inventory in the warehouse, signed cheques, or digital EFT payment tokens.
3. **Recording:** Maintaining journals, subsidiary ledgers, supplier master details, or bank reconciliations.

Transaction Cycle	Authorisation Role	Custody Role	Recording Role	Consequence if Combined
Revenue Cycle	Credit Manager approves credit limits & write-offs.	Warehouse ships goods; Cashier handles receipts.	AR Clerk posts invoices & reconciles subledger.	AR clerk could pocket customer cash and write off the receivable as a bad debt.
Expenditure Cycle	Procurement Manager issues Purchase Orders.	Receiving Clerk accepts goods; Treasurer releases EFT.	AP Clerk enters supplier tax invoices & maintains vendor master.	AP clerk could create a fictitious shell vendor, enter fake invoices, and disburse EFT to self.
Payroll Cycle	HR Manager adds staff & sets salary rates.	Treasurer approves ABA payroll bank upload.	Payroll Officer computes STP pay run & leave accruals.	Payroll officer could insert a ghost employee or inflate overtime hours and divert net pay.
IT Functions	Change Advisory Board approves code releases.	Operations / Cloud Admin deploys to production.	Developers write application code; Security Admin assigns roles.	Developer could insert unauthorised rounding-skimming code directly into production payroll.

In small Australian enterprises where limited headcount prevents full three-way segregation, management must institute **compensating controls**—such as direct owner-manager review of monthly unedited bank statements, dual-token EFT release, and independent external accountant reconciliations.

Quantitative Risk Assessment & Control Cost-Benefit Analysis

Because controls consume financial capital and employee time, management must evaluate control investments quantitatively using Expected Monetary Loss modelling:

$$\text{SLE} = \text{AV} \times \text{EF}$$

$$\text{ALE} = \text{SLE} \times \text{ARO}$$

$$\text{Net Control Benefit} = (\text{ALE}_{\text{before}} - \text{ALE}_{\text{after}}) - C_{\text{annual}}$$

Where: *SLE* is Single Loss Expectancy (expected AUD loss from one occurrence of a threat); *AV* is Asset Value (total AUD value at risk); *EF* is Exposure Factor (percentage of asset value lost per incident, $0 \le EF \le 1$); *ALE* is Annualised Loss Expectancy (expected annual loss in AUD); *ARO* is Annualised Rate of Occurrence (expected frequency of the threat per year); and C_{annual} is the annualised cost of implementing and operating the proposed control.

Worked Example 3.1: Evaluating a Supplier Master-File MFA & Verification Control

Brisbane Civil Engineering Pty Ltd faces Business Email Compromise (BEC) attacks targeting supplier BSB/bank account modifications. Each fraudulent payment diversion averages \$120,000 ($AV = 200{,}000$ AUD average batch size, $EF = 60\%$), and industry threat intelligence estimates an unprotected occurrence rate of $\text{ARO}_{\text{before}} = 0.35$ incidents per year (roughly once every three years). Management proposes implementing an automated ABN/bank-account verification service (such as Eftsure) plus mandatory out-of-band phone callback and MFA at an annual cost of $C_{\text{annual}} = 11{,}500$ AUD (\$11,500), reducing expected occurrence to $\text{ARO}_{\text{after}} = 0.03$ per year.

1. **Compute Single Loss Expectancy (SLE):** $\text{SLE} = 200{,}000 \times 0.60 = 120{,}000$ AUD (\$120,000 per incident).

DegreeLive

2. **Compute Baseline Annualised Loss Expectancy:** $\text{ALE}_{\text{before}} = 120{,}000 \times 0.35 = 42{,}000$ AUD ($42,000 per year).
3. **Compute Residual Annualised Loss Expectancy:** $\text{ALE}_{\text{after}} = 120{,}000 \times 0.03 = 3{,}600$ AUD ($3,600 per year).
4. **Calculate Net Control Benefit:**

$$\text{Net Control Benefit} = (42{,}000 - 3{,}600) - 11{,}500 = 38{,}400 - 11{,}500 = 26{,}900 \text{ AUD/year}$$

   Where: $42,000 is baseline expected annual loss, $3,600 is residual expected annual loss, and $11,500 is annualised control operating cost, yielding a net benefit of $26,900 per year.

5. **Decision:** Because the net annual benefit is strongly positive ($26,900/year), deploying the verification control is economically optimal.

3.4 General IT Controls (GITCs) & Application Controls

Auditors under ASA 315 partition IT controls into two interdependent tiers: **General IT Controls (GITCs)**, which govern the overall computing environment across all systems, and **Application Controls**, which operate inside specific business software (e.g., billing, payroll) to ensure completeness, accuracy, and validity of transactions.

General IT Controls (GITCs)

- **Logical Access & Identity Management:** Enforcing Role-Based Access Control (RBAC) aligned to the principle of *least privilege*, provisioning/de-provisioning accounts immediately upon hiring or termination, and enforcing phishing-resistant Multi-Factor Authentication (MFA).
- **Change Management & SDLC Controls:** Separating *Development*, *Test/UAT*, and *Production* environments; requiring formal peer code review, user acceptance testing, and Change Advisory Board (CAB) sign-off before migrating tax or GL logic updates into production.
- **Backup, Recovery & Business Continuity:** Implementing immutable offline/off-site backups tested periodically against two quantitative resilience targets: **Recovery Time Objective (RTO)** (maximum tolerable downtime before business interruption becomes critical) and **Recovery Point Objective (RPO)** (maximum tolerable age of data lost since the last backup snapshot).

Application Controls: Input, Processing, and Output

If GITCs fail (e.g., an unauthorised administrator disables validation rules), application controls cannot be relied upon. When GITCs are sound, application controls safeguard data integrity across three stages:

1. **Input Controls:** Prevent erroneous data from entering the database using automated edit checks:
   - *Field & Sign Checks:* Reject alphabetic characters in numeric AUD fields or negative quantities on standard invoices.
   - *Validity Checks:* Match entered Customer IDs, GL account numbers, or ABNs against active master tables.
   - *Limit & Range Checks:* Block hourly wage entries exceeding $250/hour (limit check) or transaction dates falling outside the open fiscal month (range check).
   - *Completeness Checks:* Refuse saving a tax invoice if mandatory fields (Customer ABN, Tax Code) are blank.
   - *Check-Digit Verification:* Append a mathematical parity digit to key identifiers (ABNs, TFNs, customer IDs) to catch transposition and transcription errors immediately at data entry.
   - *Batch Control Totals:* Verify batched inputs using three totals: a **Financial Total** (sum of AUD invoice amounts), a **Hash Total** (sum of a meaningless numeric field such as Customer IDs), and a **Record Count** (number of source documents).
2. **Processing Controls:** Ensure accurate computation and file updating via *run-to-run totals* (comparing batch totals after each processing step), *concurrent update locks* (preventing two clerks from allocating the same inventory unit simultaneously), and *internal header/trailer file labels*.
3. **Output Controls:** Restrict distribution of sensitive payroll and financial reports, require user reconciliation of exception reports, and log all report exports to detect unauthorised data exfiltration.

Worked Example 3.2: Australian Business Number (ABN) Modulo-89 Check-Digit Verification

Every 11-digit Australian Business Number (ABN) embeds a mathematical check mechanism enforced by the ATO and automated AIS validation scripts to block invalid supplier entries. To verify an ABN $d_1 d_2 d_3 \ldots d_{11}$, the AIS executes a weighted Modulo-89 algorithm:

1. Subtract 1 from the first (leftmost) digit d_1.
2. Multiply each of the 11 digits by its official ATO positional weight vector $W = [10, 1, 3, 5, 7, 9, 11, 13, 15, 17, 19]$.
3. Sum the 11 products and compute $S \bmod 89$. The ABN is structurally valid if and only if $S \bmod 89 = 0$.

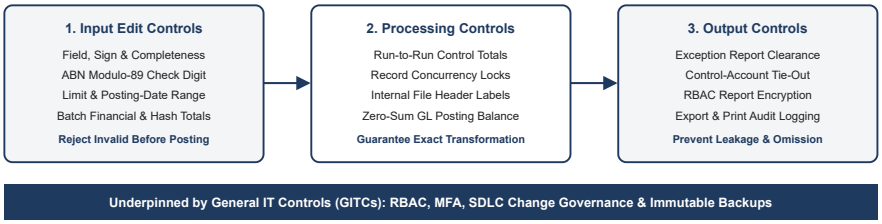
Verify Monash University's official ABN `12 377 614 012`:

- Subtract 1 from $d_1 = 1 \rightarrow 0$. Adjusted digits: $[0, 2, 3, 7, 7, 6, 1, 4, 0, 1, 2]$.
- Weighted sum:

> $$S = (0 \times 10) + (2 \times 1) + (3 \times 3) + (7 \times 5) + (7 \times 7) + (6 \times 9) + (1 \times 11) + (4 \times 13) + (0 \times 15) + (1 \times 17) + (2 \times 19)$$
>
> $$S = 0 + 2 + 9 + 35 + 49 + 54 + 11 + 52 + 0 + 17 + 38 = 267$$

- Check divisibility: $267/89 = 3$ with remainder 0 ($267 \bmod 89 = 0$). Therefore, `12 377 614 012` passes automated AIS input validation. If a clerk accidentally transposed two digits (e.g., entering `12 377 641 012`), $S = 267 - (1 \times 11 + 4 \times 13) + (4 \times 11 + 1 \times 13) = 261$, and $261 \bmod 89 = 83 \neq 0$, causing immediate rejection before saving.

Figure 3.2: Application Control Pipeline — Input, Processing & Output Gates



Worked Example 3.3: Batch Control Totals Verification in Accounts Payable

An AP clerk prepares a morning batch of four supplier tax invoices before posting to the general ledger: Supplier IDs `2041` ($1,250.00), `2088` ($3,400.00), `2115` ($890.00), and `2190` ($2,160.00). Compute the three pre-posting batch control totals and demonstrate which error each detects:

1. **Record Count:** 4 invoices. Detects an omitted or duplicated invoice record.
2. **Financial Total:** $1,250.00 + 3,400.00 + 890.00 + 2,160.00 = 7,700.00$ AUD ($7,700.00). Detects any dollar-value transposition (e.g., typing $1,520.00 instead of $1,250.00).
3. **Hash Total (Supplier IDs):** $2041 + 2088 + 2115 + 2190 = 8,434$. Although summing ID numbers has no financial meaning, if the clerk accidentally posts the $890.00 invoice to Supplier `2151` instead of `2115`, the Financial Total and Record Count still balance, yet the Hash Total shifts to $8,470 \neq 8,434$, halting the batch automatically before misposting to the wrong vendor subledger.

3.5 Australian Cybersecurity & Privacy Regulation (ASD Essential Eight & Privacy Act 1988)

Modern accounting systems operate within an increasingly stringent Australian regulatory perimeter combining technical cyber baselines with statutory data-privacy duties.

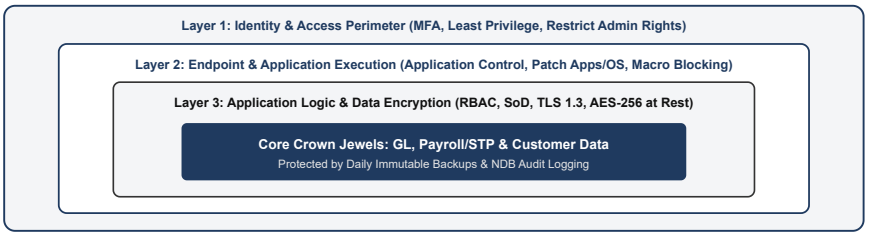
The ASD Essential Eight Maturity Model

Developed by the Australian Signals Directorate's Australian Cyber Security Centre (ACSC), the **Essential Eight** represents the baseline technical mitigation suite recommended for all Australian government and commercial organisations—and increasingly treated by ASIC and cyber insurers as a benchmark of reasonable care under Corporations Act s 180:

Essential Eight Strategy	Primary Cyber Risk Mitigated	AIS Implementation Example
1. Application Control	Execution of unauthorised malware or rogue scripts on workstations/servers.	Allowlist only signed ERP clients, Excel, and approved browsers on finance terminals.
2. Patch Applications	Exploitation of known vulnerabilities in browsers, PDF readers, and ERP plugins.	Patch internet-facing accounting portals and high-risk CVEs within 48 hours.
3. Configure MS Office Macros	Malicious VBA macros delivering banking trojans inside supplier email attachments.	Block internet-originating macros; allow only digitally signed macros in trusted finance folders.
4. User Application Hardening	Drive-by exploits via browser ads, Java, Flash, or untrusted PDF scripts.	Disable unneeded browser plugins and enforce hardened PDF rendering inside ERP viewers.
5. Restrict Admin Privileges	Attackers escalating privileges to dump payroll databases or disable audit logs.	Finance clerks operate without local admin rights; privileged ERP access uses just-in-time elevation.
6. Patch Operating Systems	Privilege escalation and worm propagation (e.g., ransomware) across servers.	Automated monthly or 48-hour emergency patching for Windows/Linux database hosts.

Essential Eight Strategy	Primary Cyber Risk Mitigated	AIS Implementation Example
7. Multi-Factor Authentication	Credential stuffing, phishing, and unauthorised cloud accounting logins.	Mandatory phishing-resistant MFA (FIDO2/authenticator) for Xero, MYOB, SAP, and VPN logins.
8. Regular Backups	Permanent data loss or extortion during ransomware encryption incidents.	Daily immutable, air-gapped cloud backups of GL/STP databases with quarterly restore drills.

Figure 3.2: Defence-in-Depth Security Architecture Aligned to ASD Essential Eight



The Australian Privacy Act 1988 (Cth) & Notifiable Data Breaches (NDB) Scheme

Accounting systems routinely store Sensitive and Personal Information—including employee Tax File Numbers (TFNs), dates of birth, medical leave certificates, and customer bank details. Under the ***Privacy Act 1988 (Cth)***, Australian Privacy Principle (APP) entities (generally businesses with annual turnover exceeding $3 million, plus health service providers and credit reporters) must comply with 13 APPs:

- **APP 1 (Open and Transparent Management):** Maintain an accurate Privacy Policy explaining how AIS personal data are collected and stored.
- **APP 6 (Use or Disclosure):** Use collected customer or payroll data strictly for the primary purpose (or a directly related secondary expectation), prohibiting unauthorised commercial resale.
- **APP 8 (Cross-Border Disclosure):** Before hosting payroll or CRM data in overseas cloud regions, take reasonable steps to ensure the foreign recipient upholds equivalent privacy protections.
- **APP 11 (Security of Personal Information):** Take reasonable steps—encryption, RBAC, MFA—to protect personal data from misuse, interference, loss, and unauthorised access, and securely destroy or de-identify records when no longer required by s 286 or tax law.

Furthermore, under the **Notifiable Data Breaches (NDB) scheme** (Part IIIC of the Privacy Act), if an AIS suffers unauthorised access or disclosure of personal information that is likely to result in *serious harm* to affected individuals and remedial action fails to prevent that harm, the entity must promptly notify both the Office of the Australian Information Commissioner (OAIC) and the affected individuals. Complementary legislation under the ***Security of Critical Infrastructure Act 2018 (Cth)*** **(SOCI)** imposes heightened cyber-incident reporting and risk-management obligations across energy, banking, transport, and cloud-infrastructure sectors.

ASD Essential Eight Maturity Progression (Levels 1 to 3)

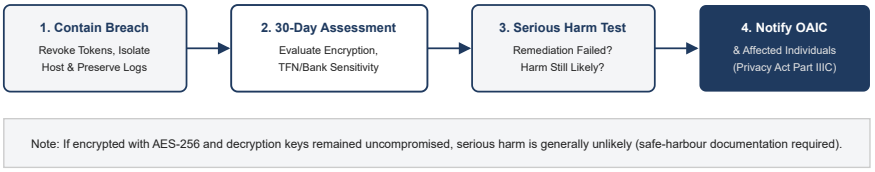
The ACSC structures Essential Eight implementation across three progressive Maturity Levels aligned to adversary sophistication: *Maturity Level 1 (ML1)* targets opportunistic commodity attackers, *Maturity Level 2 (ML2)* counters targeted ransomware and credential theft, and *Maturity Level 3 (ML3)* defends against adaptive nation-state adversaries. Australian listed companies and APRA-regulated entities typically target at least ML2 across core finance and payroll endpoints:

Control Domain	Maturity Level 1 (Opportunistic)	Maturity Level 2 (Targeted Crime)	Maturity Level 3 (Adaptive Adversary)
Multi-Factor Authentication	MFA enforced for remote access and admin portals.	MFA enforced across all cloud apps (Xero/ERP) and internal privileged steps.	Phishing-resistant FIDO2/hardware tokens mandatory for all users & admins.
Patch Applications	Patch internet-facing apps within 2 weeks (48 hrs if exploited).	Patch high-risk vulnerabilities within 48 hours using automated scanners.	Patch internet-facing & office apps within 48 hours; remove unsupported software.
Application Control	Block unapproved executables in user-profile & temp folders.	Enforce publisher/hash allowlisting across workstations and finance servers.	Full allowlisting including DLLs, scripts, and kernel drivers with cryptographic validation.
Regular Backups	Backups isolated from network; restoration tested annually.	Immutable backups encrypted & inaccessible via standard admin accounts.	Offline/immutable backups tested semi-annually against strict RTO/RPO targets.

Notifiable Data Breaches (NDB) Assessment & Escalation Workflow

Under Privacy Act s 26WH, when an organisation discovers a suspected breach—such as an exfiltrated payroll CSV containing employee TFNs and bank BSBs—it must conduct a reasonable and expeditious assessment within **30 calendar days**, documenting containment steps, likelihood of serious harm (considering encryption strength and sensitivity), and statutory notification to the OAIC.

Figure 3.3: Australian NDB Scheme Assessment & Incident Response Timeline



3.6 Computer-Assisted Audit Techniques (CAATs) & Forensic Auditing

In modern paperless AIS environments, auditors cannot "audit around the computer" by inspecting source printouts alone; instead, they apply **Computer-Assisted Audit Techniques (CAATs)** to test automated application controls directly and interrogate 100% of transaction populations.

System-Oriented CAATs for Testing Program Logic

- **Test Data Method:** The auditor prepares a synthetic batch of valid and deliberately invalid transactions (negative hours, non-existent ABN, over-limit credit orders) and processes them through a *copy* of the client's application program, comparing actual error rejections against expected outcomes without corrupting live ledgers.
- **Integrated Test Facility (ITF):** Embeds a fictitious "dummy" entity (e.g., a test department or customer account) inside the live production database so auditors can submit test transactions alongside real daily operations and filter out dummy postings prior to financial reporting.
- **Parallel Simulation:** The auditor writes an independent program (or SQL/Python script) replicating client accounting rules—such as AASB 116 depreciation or payroll PAYG tables—reprocesses actual historical client transaction files, and investigates any variance between client ledger output and simulated output.
- **Embedded Audit Modules (EAM):** Continuous auditing subroutines installed inside the ERP that automatically flag high-risk events in real time (such as manual journal entries posted after 10:00 pm on weekends or supplier bank changes exceeding $50,000).

Data-Oriented CAATs and Benford's Law Anomaly Detection

Using Generalised Audit Software (GAS) such as ACL, IDEA, or SQL analytics scripts, auditors test full population datasets for duplicates (identical invoice numbers and amounts), gaps in sequential numbering, weekend postings, and statistical digit anomalies using **Benford's Law**. In naturally occurring financial datasets spanning several orders of magnitude (such as corporate expense reimbursements or supplier invoices), leading digits are not uniformly distributed (11.1% each); rather, smaller leading digits appear far more frequently according to the logarithmic distribution:

$$P(d) = \log_{10}\left(1 + \frac{1}{d}\right), \quad d \in \{1, 2, \ldots, 9\}$$

Where: d is the first non-zero leading digit of an unmanipulated monetary amount (1 through 9); and $P(d)$ is the expected theoretical proportion of transactions beginning with digit d.

Worked Example 3.4: Forensic Benford's Law Test on Corporate Expense Claims

An internal auditor at an ASX-listed Melbourne retailer extracts $N = 2,000$ employee corporate-card expense claims where management policy mandates receipt verification and director sign-off strictly for claims of **$500.00 or more**. Using Benford's Law, compute the expected frequency of claims starting with digit $d = 1$ versus digit $d = 4$, and evaluate an observed count of 348 transactions starting with digit 4 (most clustered between $480 and $499).

1. **Theoretical Benford proportions:**
   - For $d = 1$: $P(1) = \log_{10}(1 + 1/1) = \log_{10}(2) \approx 0.3010$ (30.10%, or $2,000 \times 0.3010 = 602$ expected claims).
   - For $d = 4$: $P(4) = \log_{10}(1 + 1/4) = \log_{10}(1.25) \approx 0.0969$ (9.69%, or $2,000 \times 0.0969 = 193.8 \approx 194$ expected claims).
2. **Compare observed vs expected for $d = 4$:** Observed proportion $= 348/2,000 = 17.40\%$ versus Benford expectation of 9.69% (an excess of 154 claims).
3. **Compute standard-normal Z-statistic (incorporating continuity correction):**

$$Z = \frac{|p_{\text{obs}} - P(4)| - \frac{1}{2N}}{\sqrt{\frac{P(4)(1-P(4))}{N}}} = \frac{|0.1740 - 0.0969| - 0.00025}{\sqrt{\frac{0.0969 \times 0.9031}{2,000}}} = \frac{0.07685}{0.006615} \approx 11.62$$

Degree Live

4. **Audit conclusion:** Because $Z = 11.62 \gg 2.58$ ($p < 0.01$), the spike in leading digit 4 is statistically extreme and strongly indicates **threshold-avoidance splitting**—employees deliberately splitting larger purchases into sub-$500 claims ($480–$499) to bypass director approval controls. The auditor immediately targets all $400–$499 claims made on the same date to the same merchant for substantive testing.

3.7 Cloud Vendor Assurance (SOC 1 / SOC 2), SDLC Governance & Continuous Auditing

When Australian entities migrate accounting workloads from on-premises servers to Software-as-a-Service (SaaS) platforms, they transfer physical server administration to external cloud vendors without relinquishing statutory accountability under the *Corporations Act 2001* or *Privacy Act 1988*. Under auditing standard **ASA 402 *Audit Considerations Relating to an Entity Using a Service Organisation***, user-entity controllers and external auditors must evaluate the reliability of the cloud provider's control environment.

SOC 1 and SOC 2 Type II Assurance Reports

Rather than permitting thousands of customer auditors to inspect vendor data centres individually, major cloud AIS providers commission independent System and Organisation Controls (SOC) examinations under ISAE 3402 / ASAE 3402:

- **SOC 1 (Internal Control over Financial Reporting — ICFR):** Evaluates controls at the service organisation that are directly relevant to user entities' financial statements (e.g., payroll tax table updates, multi-tenant database isolation, and automated revenue billing logic).
- **SOC 2 (Trust Services Criteria):** Evaluates operational and cybersecurity controls across five Trust Services Criteria: *Security* (mandatory), *Availability*, *Processing Integrity*, *Confidentiality*, and *Privacy*.
- **Type I vs Type II Reports:** A *Type I* report attests only to control design at a single point in time, whereas a **Type II** report tests and attests to the *operating effectiveness* of those controls over a sustained audit window (typically 6–12 months). For substantive audit reliance, controllers require a clean SOC 1/SOC 2 Type II report and must verify that the organisation implements all **Complementary User Entity Controls (CUECs)** specified in the vendor report (such as enforcing customer-side MFA and reviewing user-access lists quarterly).

Assurance Dimension	Service Organisation Responsibility (Cloud Vendor)	User Entity Responsibility (CUEC — Client Firm)
Physical & Infrastructure Security	ISO 27001 data-centre access, hypervisor patching, AES-256 disk encryption.	Endpoint protection (ASD Essential Eight) on finance staff laptops.
Logical Access & SoD	Provide RBAC permission engine, MFA support, and immutable audit logs.	Assign least-privilege roles, revoke leavers immediately, review SoD conflicts.
Backup & Disaster Recovery	Geo-redundant database replication within Australian regions (e.g., Sydney/Melbourne).	Maintain independent archival exports for 7-year Corporations Act s 286 retention.
Tax & Statutory Logic	Maintain current ATO STP Phase 2 schemas and GST/BAS calculation templates.	Select accurate item tax codes (`GST`, `FRE`, `CAP`) and review BAS prior to lodgement.

System Development Life Cycle (SDLC) & Change-Control Gates

Even well-designed financial controls fail if unreviewed code changes enter production. Mature IT governance enforces structured SDLC stage-gates across five phases: (1) *Systems Analysis* (feasibility and requirements sign-off), (2) *Conceptual & Physical Design* (building SoD and edit checks natively into schemas), (3) *Development & Testing* (unit testing, integration testing, and User Acceptance Testing signed off by business controllers rather than programmers), (4) *Change Promotion* (independent release managers migrating approved code from staging to production with rollback plans), and (5) *Post-Implementation Review* (verifying benefit realisation and control integrity 90 days post-go-live).

Continuous Control Monitoring (CCM) Performance Trade-Offs

Contemporary internal audit teams deploy Continuous Control Monitoring scripts inside ERP platforms to flag suspicious transactions daily. However, overly sensitive anomaly thresholds overwhelm auditors with false positives ("alert fatigue"), whereas overly permissive thresholds allow genuine fraud to escape detection. Analysts calibrate rule thresholds using precision and recall metrics:

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}, \qquad \text{Recall (Detection Rate)} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

Where: *TP* (True Positives) is the number of genuinely anomalous or fraudulent transactions correctly flagged; *FP* (False Positives) is the number of legitimate transactions erroneously flagged; and *FN* (False Negatives) is the number of anomalous transactions missed by the monitoring rule.

By iteratively tuning rule parameters—for example, excluding recurring pre-approved utility direct debits from weekend-posting alerts while tightening duplicate-invoice fuzzy matching across supplier ABN and bank BSB pairs—internal auditors raise Precision without sacrificing Recall on high-materiality disbursements.

3.8 Business Continuity Planning (BCP), Disaster Recovery & Resilience Economics

Internal control encompasses not only preventing unauthorised transactions but also preserving the *availability* of the AIS during severe operational disruptions—including ransomware outbreaks, data-centre power failures, or bushfire/flood emergencies disrupting Australian regional logistics hubs. Under APRA Prudential Standard CPS 230 (*Operational Risk Management*) and ISO 22301, finance leaders align **Business Continuity Planning (BCP)** (keeping core customer billing and payroll running) with **Disaster Recovery (DR)** (restoring underlying databases and networks).

Disaster Recovery Tier Architectures

Selecting an appropriate DR architecture trades off ongoing standby infrastructure cost against acceptable downtime (RTO) and transaction-data loss (RPO):

Recovery Tier	Technical Architecture	Typical RTO	Typical RPO	Cost & Suitability
Cold Site / Tape-Cloud Restore	Empty standby facility or unprovisioned cloud tenancy; restore OS & backups manually.	48–96 hours	24 hours	Lowest monthly cost; acceptable only for non-urgent back-office ledgers.
Warm Site (Pilot Light)	Core database replicas sync periodically; compute nodes scale up on failover declaration.	4–12 hours	1–4 hours	Balanced cost; common for mid-sized wholesale/manufacturing ERPs.
Hot Site (Multi-AZ Failover)	Fully provisioned standby servers with near-real-time log shipping across regions.	< 1 hour	< 15 mins	High standby cost; required for national retail POS & high-volume e-commerce.
Active-Active Multi-Region	Simultaneous live traffic across Sydney & Melbourne availability zones with synchronous replication.	Near-zero	Zero	Highest complexity & cost; mandatory for ASX clearing & major ADIs.

Worked Example 3.5: Quantitative Disaster Recovery Tier Selection

Canberra Logistics Group Pty Ltd experiences an average of $\lambda = 0.5$ major AIS outage events per year (once every two years). During an outage, lost contribution margin and SLA penalties cost $L_{\text{hr}} = 14{,}000$ AUD/hour of downtime, and reconstructing lost unbacked transactions costs $L_{\text{data}} = 9{,}000$ AUD/hour of RPO data loss. Management compares a **Cold Site** ($C_{\text{infra}} = 24{,}000$ AUD/yr, RTO $= 48$ hrs, RPO $= 24$ hrs) against a **Warm Cloud Failover** ($C_{\text{infra}} = 145{,}000$ AUD/yr, RTO $= 4$ hrs, RPO $= 1$ hr) using expected annualised DR cost:

$$\text{Expected Annual DR Cost} = C_{\text{infra}} + \lambda\left[(L_{\text{hr}} \times \text{RTO}) + (L_{\text{data}} \times \text{RPO})\right]$$

Where: C_{infra} is the annualised infrastructure subscription cost (AUD); λ is expected annual frequency of major outages; L_{hr} is hourly business-interruption loss (AUD/hour); *RTO* is Recovery Time Objective (hours); L_{data} is hourly unbacked transaction reconstruction cost (AUD/hour); and *RPO* is Recovery Point Objective (hours).

1. **Cold Site Expected Annual Cost:**

$$24{,}000 + 0.5\left[(14{,}000 \times 48) + (9{,}000 \times 24)\right] = 24{,}000 + 0.5(672{,}000 + 216{,}000) = 468{,}000 \text{ AUD/yr}$$

2. **Warm Cloud Failover Expected Annual Cost:**

$$145{,}000 + 0.5\left[(14{,}000 \times 4) + (9{,}000 \times 1)\right] = 145{,}000 + 0.5(56{,}000 + 9{,}000) = 177{,}500 \text{ AUD/yr}$$

3. **Decision:** Although the Warm Cloud tier increases annual infrastructure spend by \$121,000 (\$145,000 vs \$24,000), it reduces expected annual total resilience cost by $468{,}000 - 177{,}500 = 290{,}500$ AUD/yr (\$290,500/year), making Warm Cloud Failover strictly superior.

3.9 ERP Role-Design Governance, Sensitive Transactions & GITC Audit Sampling

In large Australian enterprises operating multi-module ERPs, Segregation of Duties cannot be evaluated merely by inspecting job titles on an HR chart; auditors must test actual *system-level role assignments* inside the ERP security tables. Because users routinely accumulate temporary project roles over several years ("privilege creep"), Governance, Risk, and Compliance (GRC) modules scan user permission matrices continuously for toxic transaction-code combinations.

Degreelive

Toxic ERP Role Combinations and Compensating Controls

Even a single unmitigated sensitive permission pair undermines financial statement assertions across entire transaction cycles. The table below summarises critical ERP SoD conflict pairs and the compensating monitoring controls required whenever small regional branches cannot separate roles completely:

Incompatible Permission Pair	Cycle Exposure	Fraud / Error Vector	Mandatory Compensating Control
Maintain Vendor Master + Post AP Invoice	Expenditure	Create shell vendor or edit BSB and post fictitious expense voucher.	Automated daily diff report of vendor bank changes reviewed by independent Financial Controller.
Create Purchase Order + Approve Goods Receipt	Expenditure	Confirm receipt of undelivered stock to trigger supplier kickback payment.	Independent warehouse count verification and periodic physical stocktake reconciliation.
Maintain Customer Master + Post Credit Memo	Revenue	Suppress customer cash collection via fraudulent credit note write-off.	Sequential credit-memo threshold workflow requiring CFO sign-off above $1,000.
Maintain Payroll Master + Release ABA Bank File	Payroll	Insert ghost employee or alter hourly rate and disburse funds directly.	HR-only master maintenance plus dual-token treasury release against signed STP summary.
Develop Code + Migrate to Production	IT / SDLC	Insert backdoor logic altering tax rounding or bypassing approval tolerances.	Automated Git/transport logs blocking self-approval; weekly production hash verification.

Evaluating GITC Deficiencies Under ASA 315 and ASA 330

When external auditors test General IT Controls (change management, access provisioning, and privileged database logs), they apply attribute sampling to verify whether controls operated consistently across the entire 12-month financial year. Suppose an entity executed $N = 180$ ERP tax and workflow configuration changes during FY2027, and audit sampling inspects $n = 25$ randomly selected change tickets. Under professional auditing standards, finding unapproved emergency changes pushed directly to production without post-implementation sign-off increases *Control Risk*, forcing the auditor either to test compensating detective controls (such as 100% automated journal-entry population testing via CAATs) or expand substantive sample sizes under ASA 330.

Worked Example 3.6: Computing Audit Control Reliance & Substantive Risk Adjustment

An audit team assesses Inherent Risk of revenue cut-off misstatement at $\text{IR} = 80\%$ and targets an overall Audit Risk ceiling of $\text{AR} = 5\%$ under the Audit Risk Model ($\text{AR} = \text{IR} \times \text{CR} \times \text{DR}$). Compare required Detection Risk (DR) when ERP change-management GITCs are effective ($\text{CR} = 25\%$) versus ineffective ($\text{CR} = 100\%$):

$$\text{DR} = \frac{\text{AR}}{\text{IR} \times \text{CR}}$$

Where: *DR* is acceptable Detection Risk (probability substantive audit tests fail to detect a material misstatement); *AR* is overall Audit Risk; *IR* is Inherent Risk; and *CR* is Control Risk.

1. **With effective GITCs ($\text{CR} = 0.25$):** $\text{DR} = 0.05/(0.80 \times 0.25) = 0.05/0.20 = 0.25$ (25%). Moderate substantive sample sizes suffice.
2. **With ineffective GITCs ($\text{CR} = 1.00$):** $\text{DR} = 0.05/(0.80 \times 1.00) = 0.0625$ (6.25%). Because Detection Risk must tighten fourfold (from 25% down to 6.25%), the audit team must expand year-end substantive cut-off testing dramatically and deploy full-population SQL CAAT reconciliation over shipping logs and billing tables.

3.10 Whistleblower Protections, Fraud Remediation & Control Matrix Synthesis

Even the strongest preventive and automated detective controls can be circumvented through executive collusion or management override. Empirical fraud surveys consistently demonstrate that confidential employee tips detect occupational fraud more frequently than external audits alone. Under **Part 9.4AAA of the *Corporations Act 2001 (Cth)***, Australian public companies, large proprietary companies, and corporate trustees must maintain a formal Whistleblower Policy and protect eligible whistleblowers (current or former employees, contractors, suppliers, and relatives) who report suspected misconduct—including accounting manipulation, tax evasion, or cybersecurity cover-ups—against victimisation and identity disclosure.

Integrating Whistleblower Channels into AIS Monitoring

From an information-systems perspective, effective whistleblower governance requires an independent third-party reporting platform segregated from internal IT administrators (preventing compromised system administrators from inspecting server IP logs to unmask complainants), encrypted case-management workflows routed directly to the Chair of the Audit and Risk Committee, and documented forensic preservation protocols (freezing relevant ERP logs and email archives immediately upon receipt of a credible allegation).

Degree Live

Comprehensive Preventive, Detective & Corrective Control Synthesis

Synthesising Module 3, controllers classify organisational safeguards across all three temporal layers to eliminate single points of failure:

Threat Vector	Preventive Control	Detective Control	Corrective Control
Unauthorised Cloud Login	Phishing-resistant FIDO2 MFA & IP geo-fencing.	SIEM impossible-travel & failed-login alerts.	Automated session revocation, credential reset & NDB assessment.
Fictitious Vendor Payment	SoD (Vendor Master vs AP) & ABN Modulo-89 validation.	Duplicate BSB/employee cross-match & Eftsure alerts.	Bank recall request, account freeze & fidelity insurance claim.
Ransomware Encryption	ASD Essential Eight Application Control & macro block.	Endpoint Detection & Response (EDR) file-entropy alerts.	Restore clean ERP snapshot from immutable air-gapped backups within RTO.
Manual Journal Override	Maker-checker workflow & locked closed periods.	CAAT weekend/after-hours & Benford's Law screening.	Audit Committee investigation, reversing JV & disciplinary sanction.

DegreeLive