2025/08/05

RISK MANAGEMENT: CONTROLS

Setting up controls in risk management involves identifying, assessing, and implementing measures to mitigate risks that could negatively impact an organisation's objectives. Here's a structured approach to setting up effective controls:

A common risk treatment option is Reduction; this applies to unacceptable risks that cannot be eliminated/avoided. Reduction is a method to manage active risks through defined control measures that diminish the risk and its impact to a tolerable level.

Control Measures

Controls can be:

- **Preventive** (stop risks before they occur, e.g., firewalls for cybersecurity).
- **Detective** (identify risks early, e.g., audits, monitoring systems).
- **Corrective** (mitigate damage after an event, e.g., disaster recovery plans).
- **Directive** (policies & training to guide behaviour, e.g., compliance training).

Select controls based on cost-effectiveness and feasibility.

A. Preventative Controls

These are proactive measures designed to stop that risk from occurring before it has any impact. Ultimately aimed at eliminating or reducing the prevalence of a risk event before it happens, rather than reacting after the fact.

Types

Preventative controls can be categorised into:

1. Administrative (Policy-Based) Controls
    - Policies & Procedures – Clear rules that guide behaviour (e.g. "No personal devices on the corporate network").
    - Approval Processes – Requiring authorisation before actions (e.g. purchase approvals).
    - Separation of Duties – Splitting tasks among employees to prevent fraud (e.g. the person who approves payments shouldn't also record them).
    - Training & Awareness Programmes – Educating employees on security, compliance, and risk avoidance.

2. Physical Controls
    - Access Restrictions – Keycards, biometric scanners, and locked doors to
    - prevent unauthorised entry.
    - Surveillance Systems – Cameras and security personnel to deter theft or
    - misconduct.
    - Environmental Safeguards – Fire suppression systems and backup generators to prevent disasters.

3. Technical (IT & Cybersecurity) Controls
    - Authentication Mechanisms – Passwords, multi-factor authentication (MFA), and biometrics to prevent unauthorised access.
    - Firewalls & Encryption – Blocking malicious traffic and securing sensitive data.

- Patch Management – Regularly updating software to prevent IT vulnerabilities.
- Whitelisting/Blacklisting – Allowing only approved applications/websites to run.

Best Practices for Implementing Preventative Controls

1. Risk-Based – Focus on high impact, high likelihood risks first.
2. Layered Defence – Combine multiple controls (e.g. firewalls + MFA + employee training).
3. Automation – Use AI and monitoring tools to enforce policies in real-time.
4. Regular Testing – Conduct penetration tests, audits, and simulations to ensure controls work.
5. Employee Involvement – Foster a culture of compliance through training and clear communication.

When Are Preventative Controls Most Effective?

- Before risk materialises (e.g. background checks to avoid hiring risks).
- When the cost of failure is high (e.g. safety protocols in nuclear plants).
- Regulated industries (e.g. POPIA, Companies Act, compliance).

Limitations

- Can be expensive to implement (e.g. advanced cybersecurity systems).
- May create operational friction (e.g. too many approval steps slowing workflows).
- Not 100% foolproof and should be paired with detective & corrective controls.

B. Detective Controls

Detective controls are mechanisms designed to identify and uncover risks, breaches, or anomalies after they occur but before they cause significant damage. Unlike preventative controls (which stop risks from happening), detective controls

focus on early detection, allowing your organisation to respond quickly and minimise impact.

Detective controls are a critical second layer in risk management, working alongside preventative and corrective controls. They act as an early warning system, helping organisations mitigate damage before it escalates.

Types

1. Monitoring & Surveillance

- Log Analysis – Reviewing system, application, and security logs for unusual activity (e.g. unauthorised access attempts).
- Real-Time Alerts – Automated notifications for suspicious transactions or network intrusions (e.g. SIEM tools like Splunk or ManageEngine Log360).
- CCTV & Physical Monitoring – Video surveillance to detect theft, workplace violations, or safety hazards.

2. Audits & Inspections

- Internal Audits – Periodic reviews of financial records, IT systems, or operational processes to detect fraud or inefficiencies.
- External Audits – Independent assessments to verify compliance.
- Inventory Checks – Physical counts to detect discrepancies.

3. Reconciliation & Exception Reporting

- Financial Reconciliation – Comparing bank statements with internal records to detect fraud or errors.
- Exception Reports – Flagging transactions that deviate from norms (e.g. unusually large payments, odd login times).

4. Intrusion Detection Systems (IDS) & Anomaly Detection

- Network IDS (NIDS) – Monitors traffic for malicious patterns (e.g. malware, DDoS attacks).

- Host-Based IDS (HIDS) – Detects suspicious activity on individual devices (e.g. unauthorised file changes).
- User Behaviour Analytics (UBA) – Uses AI to spot abnormal employee actions (e.g. unauthorised data transfer).

5. Vulnerability Scans & Penetration Testing

- Automated Scans – Tools like Nessus or Qualys scan systems for security weaknesses.
- Red Teaming – Ethical hackers simulate attacks to find gaps before criminals do.

Best Practices for Implementing Detective Controls

1. Automate Where Possible – Use AI and machine learning to detect patterns humans might miss.
2. Set Clear Thresholds – Define what constitutes an "anomaly" (e.g. transactions over R50,000 flagged for review).
3. Regular Reviews – Schedule periodic audits and log analyses (not just after incidents).
4. Integrate with Response Plans – Ensure detective controls trigger corrective actions (e.g. freezing accounts after fraud detection).
5. Balance Privacy & Monitoring – Avoid excessive surveillance that may violate employee trust or regulations.

When Are Detective Controls Most Effective?

- For risks that can't be prevented from inception (e.g. insider threats, sophisticated cyberattacks).
- In highly regulated industries (e.g. financial services require fraud detection).
- When real-time response is critical (e.g. detecting a ransomware attack before it spreads).

Limitations

- Reactive by nature – Doesn't stop risks, only identifies them.
- Can generate false positives – Requires tuning to avoid alert fatigue.
- Resource-intensive – May need dedicated teams (e.g. analysts for cybersecurity).

C. Corrective Controls in Risk Management

Corrective controls are measures designed to mitigate damage, restore operations, and prevent recurrence after a risk event has occurred. Unlike preventative (stop incidents) or detective (identify incidents) controls, corrective controls focus on response and recovery.

Types

1. Incident Response & Recovery

- Disaster Recovery Plans (DRP) – Procedures to restore IT systems after outages (e.g. ransomware attacks, server failures).
- Business Continuity Plans (BCP) – Strategies to maintain critical operations during disruptions (e.g. backup sites, emergency protocols).
- Incident Response Teams (IRT) – Dedicated teams to contain breaches (e.g. cybersecurity IRT isolating infected systems).

2. Root Cause Analysis (RCA) & Problem Resolution

- 5 W's Analysis – A technique to drill down to the underlying cause of an issue (What, When, Where, Who and Why).
- Fishbone Diagrams – Visual tools to identify contributing factors (e.g. people, processes, technology).
- Patch Management – Deploying software updates to fix vulnerabilities after an exploit.

3. Compensation & Remediation

- Insurance Claims – Financial recovery for losses (e.g. property damage, cyber incidents).

- Customer Refunds/Compensation – Addressing service failures (e.g. flight cancellations, product recalls).
- Legal Actions – Pursuing restitution from responsible parties (e.g. litigation against negligent vendors).

4. Process Improvements

- Policy Updates – Revising procedures to prevent repeat incidents (e.g. stricter access controls after a data breach).
- Employee Retraining – Addressing human errors through additional education (e.g. phishing awareness after a security lapse).
- System Upgrades – Replacing faulty equipment or outdated software.

Best Practices for Corrective Controls

1. Predefined Playbooks – Document step by step response procedures for common incidents.
2. Cross-Functional Coordination – Ensure IT, legal, PR, and operations teams align during crises.
3. Post-Incident Reviews – Conduct "lessons learned" sessions to refine future responses.
4. Automated Recovery Tools – Use backup automation, failover systems, and self-healing IT infrastructure.
5. Regulatory Compliance – Align actions with requirements (e.g. POPIA breach notifications within 72 hours).

When Are Corrective Controls Most Critical?

- After high impact incidents (e.g. data breaches, natural disasters).
- When systemic weaknesses are exposed (e.g. repeated equipment failures).
- To meet legal/contractual obligations (e.g. compensating affected customers).

Limitations

- Can be expensive (e.g. product recalls, litigation).
- May not fully reverse damage (e.g. reputational harm from a breach).
- Dependent on detection speed – Slow response worsens outcomes.

Remember

- Corrective controls are reactive but essential for resilience.
- They work best when integrated with preventative and detective controls in a layered defence.
- Continuous improvement is vital; each incident should strengthen future risk posture.

D. Directive Controls

Directive controls are governance measures that guide behaviour and establish expected standards through policies, procedures, and training. Unlike preventative (block risks) or detective (identify issues) controls, directive controls focus on ensuring compliance and aligning actions with organisational objectives.

Types

1. Policies & Standards

- Code of Conduct – Defines ethical expectations (e.g. anti bribery, conflicts of interest).
- Information Security Policies – Mandates for data handling (e.g. password complexity rules).
- Regulatory Compliance Frameworks – Ensures adherence to laws (e.g. OHSA, FICA, CPA).

2. Procedures & Guidelines

- Standard Operating Procedures (SOPs) – Step by step instructions for critical tasks (e.g. invoice approvals, IT change management).
- Work Instructions – Detailed guides for specific roles (e.g. machine operation in manufacturing).

3. Training & Awareness Programmes

- Onboarding Training – Educates new hires on compliance and safety protocols.
- Cybersecurity Awareness – Phishing simulations and secure coding workshops.
- Certification Requirements – Mandatory training for high-risk roles (e.g. forklift operators, financial advisors).

4. Supervision & Sign Off

- Managerial Approvals – Required for high stakes decisions (e.g. budget allocations, system access).
- Checklists – Ensures critical steps aren't missed (e.g. preflight inspections in aviation).

Best Practices for Directive Controls

1. Clear Documentation – Policies should be concise, accessible, and regularly updated.
2. Role Specific Training – Tailor programmes to job functions (e.g. finance teams need fraud detection training).
3. Enforcement Mechanisms – Pair with detective controls (audits) and corrective actions (penalties for noncompliance).
4. Leadership Endorsement – Executives must model compliance (e.g. following travel expense rules).
5. Continuous Reinforcement – Use quizzes, newsletters, and refresher courses to sustain awareness.

When Are Directive Controls Most Effective?

- For culture driven risks (Conduct Risk) (e.g. ethical misconduct, safety lapses).
- Regulated industries (e.g. finance, healthcare, aviation).
- Where human error is a major factor (e.g. data entry mistakes, miscommunication).

Limitations

- Dependent on adherence – Employees may bypass or ignore policies.

- Can become outdated – Regular reviews are needed to reflect new risks / regulations.
- May create bureaucracy – Excessive red tape can slow operations.

Remember

1. Directive controls set the "rules of the game" through governance and education.

2. They work best when combined with other controls:
   - Preventative (e.g. access restrictions support password policies).
   - Detective (e.g. audits verify policy compliance).
   - Corrective (e.g. retraining after violations).

3. Tone at the top matters – Leadership must prioritise and reinforce directives. Controls should always be proportional to the risk, avoid over controlling minor risks or under controlling major ones.

Cyclopedic Consulting specialises in proactively managing your organisation's uncertainty by establishing robust risk controls tailored to your operations. Whether you're building your risk management function from the ground up or strengthening existing processes, we ensure your controls are not only effective but also integrated seamlessly into your business strategy.

By **Adv. Sannah Pooe** 2025/08/05