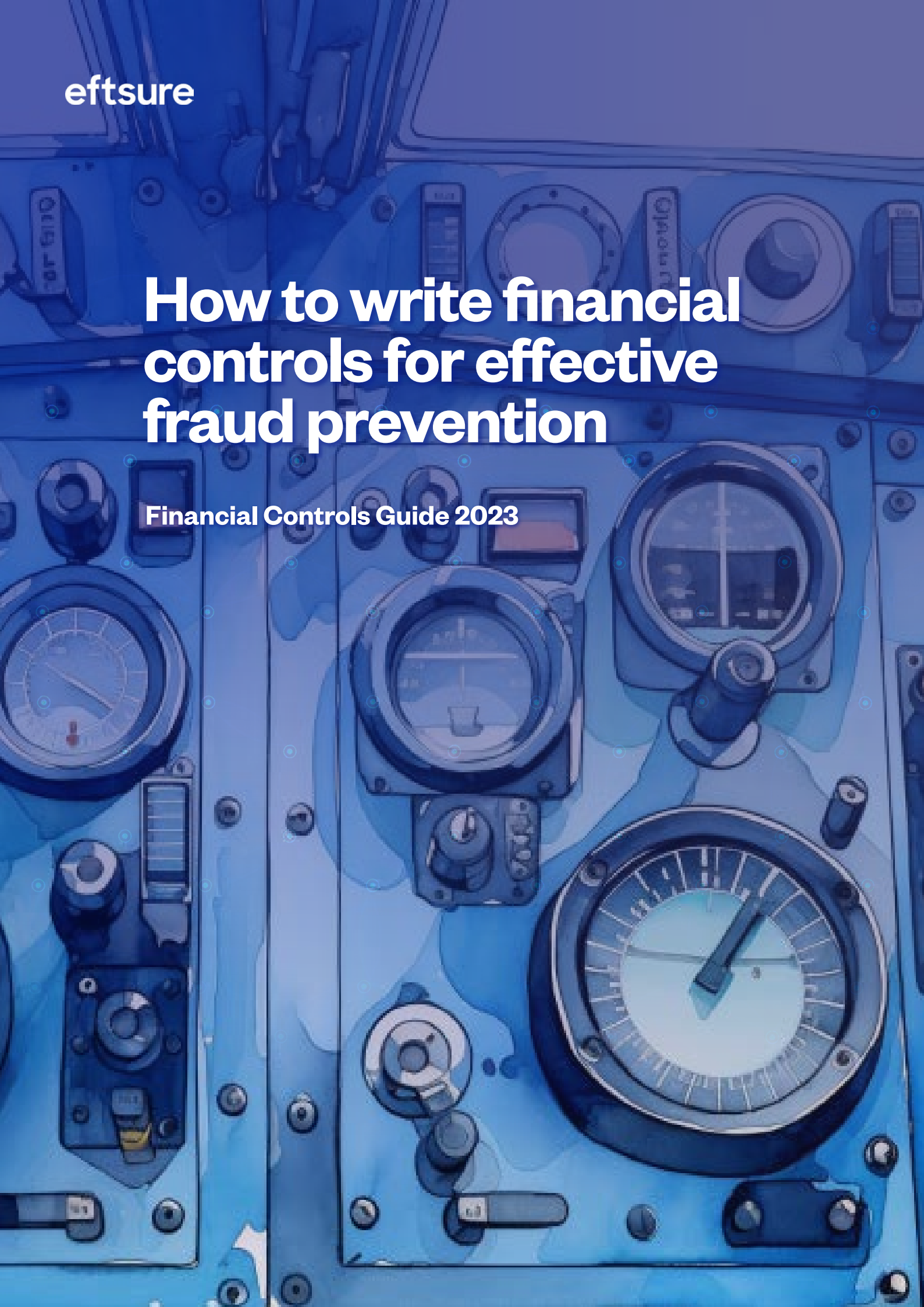
eftsure

How to write financial controls for effective fraud prevention

Financial Controls Guide 2023



Contents

eftsure

Introduction

Amid rapid digitisation, effective fraud prevention requires more than financial controls designed for an analogue world.

Cyber-criminals are becoming increasingly sophisticated with their scams, leveraging technology to refine their tactics.

As cyber-crime and data breaches continue to rise worldwide, CFOs must stay ahead of the game to protect their organisations from potential losses.

Lets take a look at this challenging landscape.

Key Findings

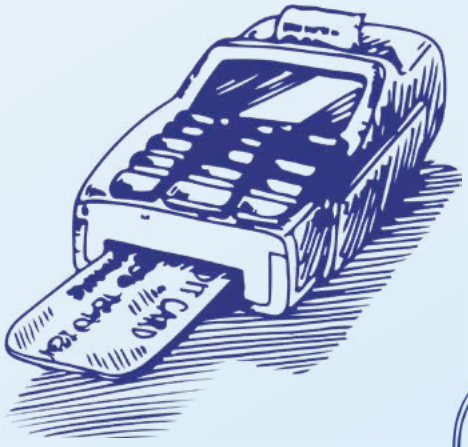
In 2021, as the economic recovery from the pandemic began, spending on Australian cards rose by **8%** **and the overall value of card fraud increased by 5.7%.**

Among victims able to identify how their details were obtained, most cited the internet **(33.3%)**, followed by card details copied or obtained during use **(15.1%)** & in person **(5.8%)**.

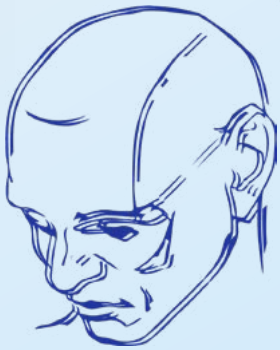
Of those who were victims of payments fraud in 2022, nearly half **(44%)** **were unsuccessful in recouping any of the stolen funds.**

When looking to report payments fraud, nearly **80%** **of organisations are most likely to seek assistance from their banking partners for guidance.**

5.7%
[1] Card fraud increase in 2021



15.1%
[2] Card details copied or obtained during use



5.8%
[1] Victims of fraud in person

1 - Australian Payments Network; Australian Payment Fraud 2022 report

2 - Australian for financial professionals; AFP Payments fraud and control survey 2024 report

eftsure

Financial professionals must stay ahead of these threats and be vigilant in continually updating and enhancing their controls. This could include strengthening internal processes, implementing oversight strategies or introducing technologies to detect anomalies.

By having comprehensive financial controls in place, organisations can reduce the risk of fraud, errors and losses due to negligence or malfeasance.

These controls must ensure the accuracy, reliability and integrity of financial data while fostering transparency, accountability, and trust – and they need to do all of this within a fast-evolving threat landscape.

If controls are ignored and prove to be inadequate, organisations might face severe consequences, such as financial losses, reputational damage and legal ramifications. By proactively implementing preventive measures, you can safeguard your financial assets in an increasingly digital world.

5.7%
[1] Card fraud increase in 2021

15.1%
[2] Victims card details copied or obtained during use

44%
[2] Of all victims nearly half were unable to recoup any of the stolen funds

5.8%
[1] Victims of fraud in person

33.3%
[1] Internet cited victims

80%
[2] Organistaions see assistance from their banking partners for guidence

1 - Australian Payments Network; Australian Payment Fraud 2022 report

2 - Australian for financial professionals; AFP Payments fraud and control survey 2024 report

eftsure

To get started, this comprehensive guide offers step-by-step instructions.

Eftsure's Approach To Oversight And Governance

eftsure


1
RISK AND VULNERABILITIES
2
DESIGNING CONTROL OBJECTIVES
3
IDENTIFYING CONTROL ACTIVITIES
4
DOCUMENTING POLICIES AND PROCEDURES
5
IMPLEMENTING CONTROL ACTIVITIES
6
MONITORING AND EVALUATION
7
REVIEWING AND IMPROVING

eftsure

Risk and vulnerabilities

Strong controls start with a thorough understanding of your risks. And that starts with an understanding of the organisation itself.

The first step in designing effective financial controls is identifying the potential risks and vulnerabilities in your organisation's financial processes. When designing financial control objectives, management needs a deep understanding of their organisation's operations, processes and risk profile. Begin with a thorough risk assessment.

This can be scheduled once every year or once every six months to keep up with the threat landscape.

As you evaluate each risk, include additional columns to identify potential new risks stemming from material weaknesses or significant IT deficiencies.

These columns should indicate the individuals responsible for each specific process, the individuals who conduct inspections, proposed solutions and a timeline of all relevant actions (plus each action's owner).

Management and IT teams should collaborate on this assessment.

Other best practices in identifying control weaknesses include:

Documenting and analysing control procedures

Regularly training appropriate stakeholders on control hygiene

Conducting scheduled audits

Reviewing and listening to feedback from stakeholders

Designing control objectives

Once the risk assessment is complete, it's time to establish control objectives. Control objectives define the desired outcomes of your financial controls.

They should align with your organisation's overall goals and values, ensuring that the controls serve a specific purpose. Control activities include implementing or updating policies, procedures and guidelines that define how financial transactions are authorised, recorded and approved. To get you started, some examples of control objectives can include:

- **Safeguarding financial assets**
- **Ensuring data integrity**
- **Preventing unauthorised transactions**

Designing control objectives

OBJECTIVE 1
Safeguarding assets

Safeguarding assets is a critical control objective. This involves implementing measures to protect physical and digital assets from unauthorised access, theft or misuse. It may include measures like restricted access to sensitive areas, secure storage for important documents and robust cybersecurity protocols.

OBJECTIVE 2
Ensuring data integrity

Data integrity is vital for accurate financial reporting and decision-making. Establish efficient controls that verify the accuracy and completeness of financial data, preventing unauthorised alterations or manipulations. Regular data backups, access controls and data validation procedures are examples of measures that contribute to data integrity.

OBJECTIVE 3
Preventing unauthorised transactions

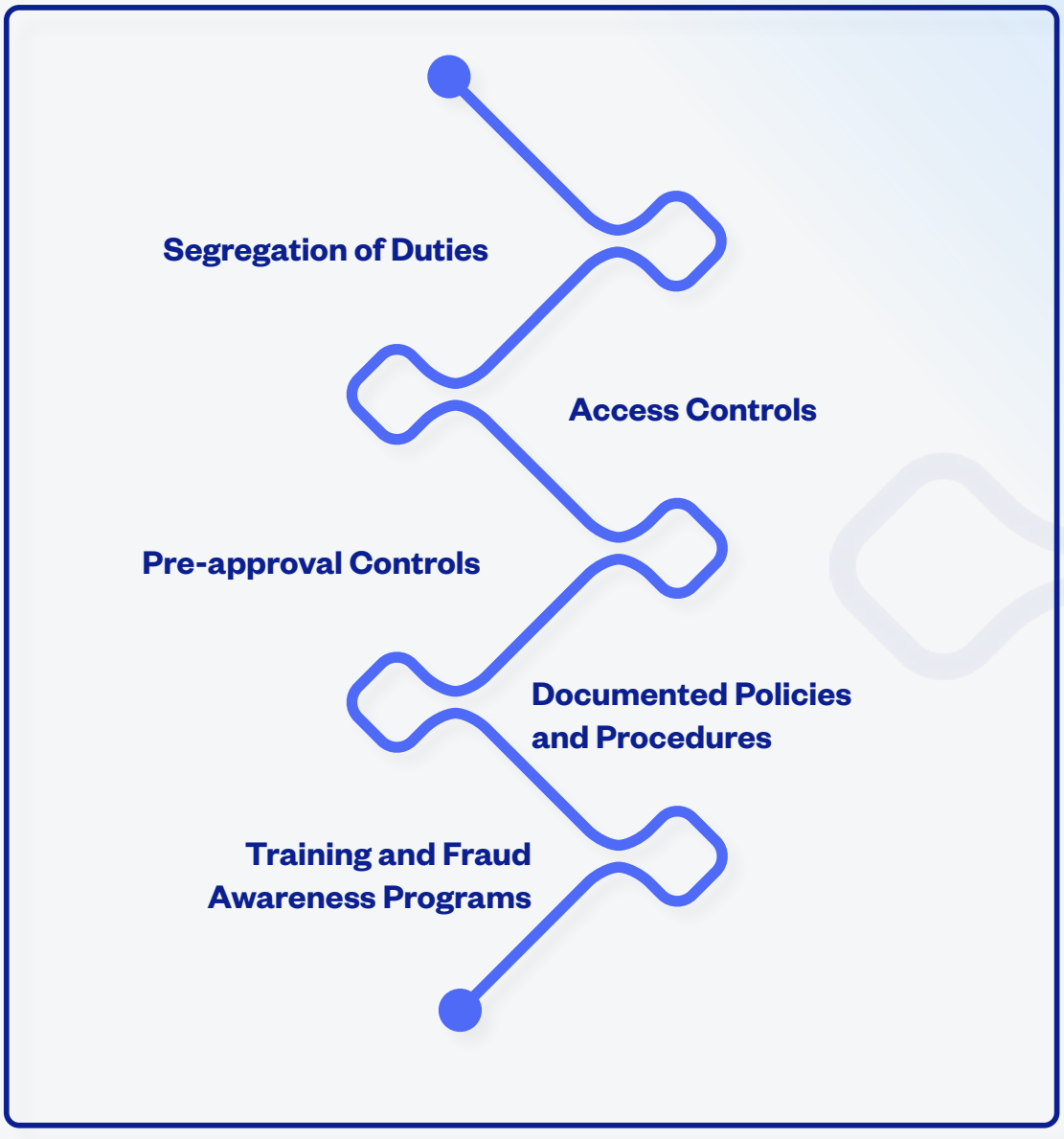
When it comes to risks like cyber-crime and internal or external fraud, unauthorised transactions are one of your biggest vulnerabilities.

Controls that detect and prevent unauthorised transactions will help guard against a wide range of malicious activity, like fictitious vendor schemes or payroll fraud. Segregation of duties, dual authorisation requirements and transaction monitoring systems can help mitigate the risk of these transactions.

Identifying control activities

Control activities are assigned to address the risks identified in the initial phase. Once you've identified which controls are important, then you need to test them and determine the effectiveness of each control process. Controls can be categorised into three groups: preventative, detective and corrective. And, within these categories, they can either be manual or automated. **Here are several control measures to consider:**

PREVENTATIVE CONTROLS



SEGREGATION OF DUTIES

Ensures that no single individual has dominion over an entire financial process. By separating responsibilities among multiple employees, organisations can create a system of checks and balances, reducing the risk of fraudulent activities. For example, the person responsible for recording financial transactions should not be the same person responsible for authorising or approving those transactions.

ACCESS CONTROLS

Mechanisms put in place to regulate and restrict access to sensitive information, systems or resources within an organisation. This ensures that only authorised individuals can perform certain actions or access sensitive data like credit card information, personal information or login credentials.

PRE-APPROVAL OF ACTIONS AND TRANSACTIONS

Authorisation or permission before carrying out specific activities of transactions. This might include actions like hiring a new employee or initiating a financial transaction. Stakeholders must go through a formal approval process before they can proceed – it's a good example of a mix of automation and manual work, since automation can help enforce and streamline approval workflows even though a human employee is ultimately making the decisions.

DOCUMENTED POLICIES AND PROCEDURES

Documentation that explains relevant steps, guidelines and rules for employees. It ensures that tasks are performed accurately, consistently and in line with the organisation's objectives and regulatory requirements. This becomes a foundational basis for training, compliance and internal audits. Regularly reviewing these policies and procedures is key.

TRAINING AND FRAUD AWARENESS PROGRAMS

By equipping employees with knowledge and awareness, organisations can empower AP teams to play an active role in identifying and preventing fraud. You'll want to make sure they understand control processes, systems and tools, but they also need to be aware of cyber threats like phishing tactics and BEC attacks. Regular workshops, quizzes and information sessions can help.

Detective controls

Data analytics and monitoring. Examining and analysing large datasets can identify anomalous patterns and potentially fraudulent activities. This usually involves specialised software that can process data pulled from multiple sources. For example, Eftsure identifies anomalies by cross-matching the supplier payments against its database of verified supplier details.

Regular financial reviews. Routinely evaluating financial records, transactions and reports is another great way to detect anomalies. During the review process, financial records and transactions are scrutinised to ensure they're following accounting standards.

Internal and external audits. Internal audits can be conducted by the internal audit function – that is, those who are responsible for evaluating and monitoring the effectiveness of internal controls, risk management practices and more. Meanwhile, "external" actors like audit firms or certified public accountants (CPAs) can conduct audits as neutral third parties. Both approaches play a crucial role in evaluating the effectiveness of controls, risk management and financial reporting.

Corrective controls

Incident reporting and investigation

Incident reporting and investigation. Employees or relevant stakeholders need both formal and informal channels to report any observations or suspected incidents to the appropriate channels or authorities. Reporting should trigger an investigation to gather relevant information, evidence and facts regarding the incident.

Disciplinary measures

Disciplinary measures. The purpose ofdisciplinary measures is to establish a clear and consistent framework for addressing and deterring bad behaviour within the organisation. They should be applied fairly, consistently and in accordance with applicable laws and organisational policies. And they should aim to deter malicious or reckless behaviour, not simply the type of good-faith human error that often comes up during highly manual workflows or hectic periods of work.

Software patches

Software patches. Regularly patching software helps maintain the security and integrity of internal systems, enabling IT teams to minimise software vulnerabilities that could be exploited by cyber-criminals.

High-profile attacks like those on Optus, Medibank, Latitude Financial and Coles illustrate that cyber-criminals are constantly looking for ways to squeeze ill-gotten money out of organisations.

And, when data breaches and ransomware attacks occur, there's a good chance that stolen data can end up in the hands of scammers – the very scammers who might be looking to target your organisation next.

As a financial leader, you and your team are the last line of defence between these scammers and your organisation's money. One of your best defences will be strong, updated controls, ones that are specifically designed to minimise the risk of today's digital fraud.

Across all forms of fraud, controls such as segregation of duties and call-back controls have proven to be effective in preventing and detecting malicious activity.

Another proven approach?

Automating and standardising certain control processes, which removes the risk of employees making good-faith errors or skipping important steps.

Manual versus automated controls

It's important to note that not all controls are good candidates for automation.

For example, certain corrective controls – like implementing new policies – may require careful contextual reasoning, which a human employee is better equipped to do.

The key to having effective financial controls is to integrate various components and implement a combination of manual and automated controls that align with the organisation's requirements.

Once you've determined what controls are going to look like and how they're going to function, it's vital to communicate these changes and ensure employees are aware of the appropriate steps in a process. Equally important is ensuring that every member of your **Accounts Payable (AP) team** comprehends these changes and understands the reasons behind their implementation.

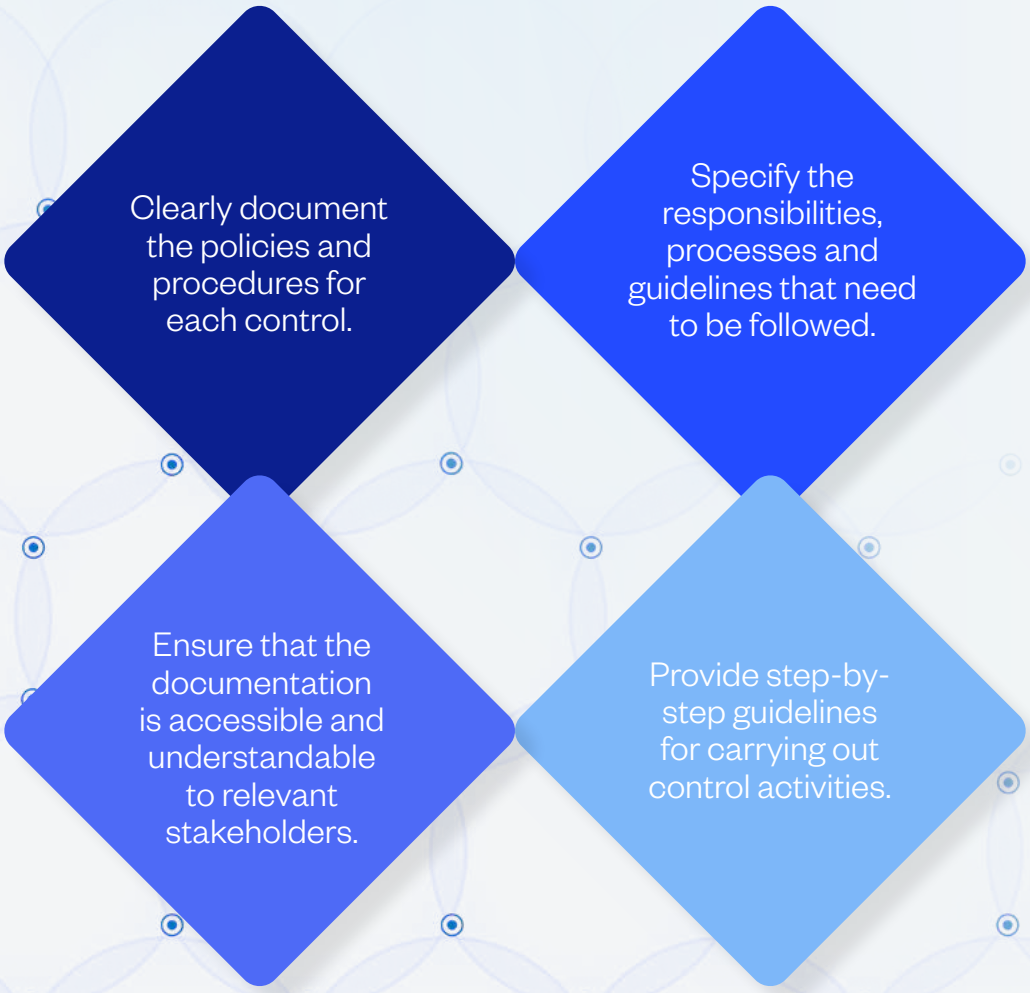
Teams are far more likely to support changes when they understand what's at stake and how changes can protect them.

Once you've decided which controls to implement, the next step is to document the chosen controls, including their objectives, procedures and owners.

Documenting policies and procedures

Documented financial controls promote transparency and help ensure that everyone's on the same page, especially the stakeholders and employees who will be most impacted by new procedures.

During this phase, you should:



By putting these details into writing, it becomes easier for stakeholders to understand the purpose and expected outcome of each control, aligning everyone around an agreed approach.

Implementing control activities

Once the control objectives are defined and documented, it's time to implement control activities.

Control activities are the specific procedures and actions that enforce financial controls.

You can start by developing a comprehensive plan outlining the timeline, resources and responsibilities for implementing the chosen controls.

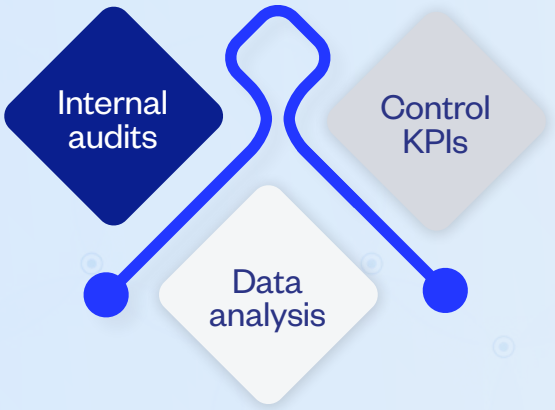
This plan should consider any dependencies, potential challenges and the necessary coordination with different teams or departments.

The Department of Finance provides a sample template for preparing a schedule of activities and tasks.

Monitoring and evaluation

Financial controls should be continuously monitored and evaluated to ensure their effectiveness. Regular assessments and audits help identify control weaknesses, policy non-compliance and emerging risks. By regularly monitoring and testing the effectiveness of the controls, you can identify any vulnerabilities or gaps and take corrective actions as needed.

Start your monitoring and evaluation by conducting the following:



1: Internal audits

Internal audits play a crucial role in evaluating the adequacy and effectiveness of financial controls.They provide an independent and objective assessment of control systems, identifying any gaps or deficiencies that require attention. Conduct regular internal audits to maintain control integrity.

2: Data analysis

Leverage data analysis techniques to identify patterns, anomalies, or suspicious activities. Implement automated monitoring systems that analyse financial transactions, vendor records or employee activities to detect potential fraud indicators. Data analysis can provide valuable insights and prompt further investigation if necessary.

3: Key performance indicators

Define and track relevant KPIs to assess the effectiveness of financial controls. KPIs can include metrics such as the number of control failures, detection rates of fraudulent activities, response times to control incidents or any other measurable factors that provide insights into control performance.

Reviewing and improving

The last phase in creating effective financial controls is continuously refining your controls. According to the Australian Securities and Investments Commission (ASIC), firms should increase their use of internal control reviews.

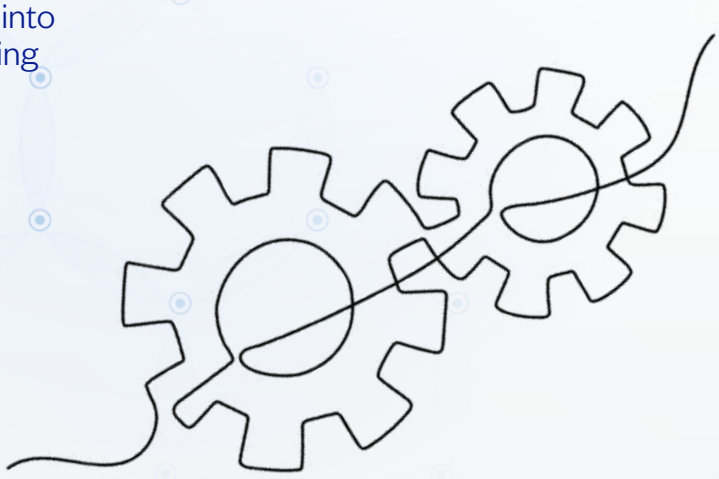
It's best practice to review and improve financial controls regularly. However, that frequency depends on your organisation's size and objectives. To get started, here are some considerations:

Annual reviews.
Conducting a comprehensive review of financial controls at least once a year is common practice. This allows for a thorough assessment of control design, implementation, and effectiveness.

Continuous monitoring.
Ongoing monitoring processes and data analytics can help identify control weaknesses or emerging fraud risks. Continuous monitoring allows for real-time insights into control performance, enabling timely adjustments and improvements as needed.

Internal audit cycles.
Aligning financial control reviews with the internal audit cycle can be beneficial. Internal audits often include evaluations of financial controls, and conducting reviews in conjunction with these audits can streamline the process. These cycles are determined by the organisation's internal audit function and management.

Feedback and incident analysis.
Incorporate feedback from employees, auditors, or stakeholders regarding control effectiveness or incidents. Analysing control-related incidents can reveal areas for improvement and guide the refinement of controls.



Remember that the goal is not just to review financial controls but also to continually improve them.

By staying proactive and responsive to changes, organisations can adapt their controls to evolving risks and strengthen their overall control framework.

eftsure

eftsure

Strengthen your financial controls with Eftsure today.

Request a demo

1300 985 967 | sales@eftsure.com.au