NSW Treasury

Compliance Incident Policy

TIPP5.15

September 2023

Acknowledgement of Country

We acknowledge that Aboriginal and Torres Strait Islander peoples are the First Peoples and Traditional Custodians of Australia, and the oldest continuing culture in human history.

We pay respect to Elders past and present and commit to respecting the lands we walk on, and the communities we walk with.

We celebrate the deep and enduring connection of Aboriginal and Torres Strait Islander peoples to Country and acknowledge their continuing custodianship of the land, seas, and sky.

We acknowledge the ongoing stewardship of Aboriginal and Torres Strait Islander peoples, and the important contribution they make to our communities and economies.

We reflect on the continuing impact of government policies and practices and recognise our responsibility to work together with and for Aboriginal and Torres Strait Islander peoples, families, and communities, towards improved economic, social and cultural outcomes.

Artwork:
Regeneration by Josie Rose

Version	
Document number TIPP 5.15	Version number: 4.0
Original issue date	Aug/ 2016
Current revision date	Sep/2023
To be reviewed on	Aug/2025

Current revision material updates include:
• Updated policy using new Treasury brand Templates. • Various minor updates to wording / fields where relevant • Enhanced and clarified definition of incident in 'Incident Definition' section 1.2 • Added 'Incident Reporting' section 2.1.3 • Added 'Data, Privacy, and Confidentiality' section 2.1.4 • Added 'Incident Escalation' requirements in 'Verification' section 2.2 • Added 'Protocols of engagement' section 4 • Added 'Protecht Reporting Input Guidance' Appendix B • Added 'Incident Classification Matrix' Appendix C

Contact details	
Name: Martin Maerzinger	Position: A/Director of Audit & Risk
Branch: Risk, Compliance and Audit	Division: Financial Management and Services Financial and Operations
	Email: risk@treasury.nsw.gov.au

Contents

Preface

NSW Treasury aims to operate in an open and collaborative culture with respect to incident reporting. An organisation's understanding of the root cause of an incident is imperative to learn from previous experiences to increase controls where appropriate and to prevent recurrence. The Treasury Executive Board (TEB) and Audit and Risk Committee (ARC) need to have visibility and awareness of notifiable or material compliance and risk events, as well as potential systemic or emerging issues.

This document sets out Treasury's policy for the management of compliance incidents as well as the responsibilities and processes that have been established to give effect to the Policy.

It is the responsibility of the relevant Executive Director for reporting and communication of compliance and risk incidents in their given business area. All members of Treasury staff are responsible for following the guidelines contained in the NSW Treasury Compliance Incident Policy with respect to the identification, management, and reporting of compliance and risk incidents.

This Policy applies to all staff including contractors and consultants working within Treasury.

Michael Coutts-Trotter

Secretary

NSW Treasury

August 2023

Note

General inquiries concerning this document should be initially directed to:

Risk, Compliance & Audit, NSW Treasury; risk@treasury.nsw.gov.au.

This publication can be accessed from the Treasury's website (www.treasury.nsw.gov.au).

This is an internal Treasury policy, published to support our commitment to transparency and accountability. As such, it may contain URLs to internal Treasury resources that may not be externally available at this time. Requests made under the *Government Information (Public Access) Act 2009* will be assessed through standard processes.

1 Introduction

1.1 Purpose

This Compliance Incident Policy (Policy) outlines the process by which NSW Treasury (Treasury) manages potential compliance failures. This Policy forms part of Treasury's Compliance Management Framework, and therefore should be read in conjunction with this document along with the Risk Management Framework.

This Compliance Incident Policy's objective is to:

- Ensure that each Division of NSW Treasury has a consistent approach to the management of risk and compliance incidents – to clearly document processes in place for employees to identify and a record incidents incident.
- Ensure effective management and reporting of compliance and risk incidents to aid and mitigate against adverse compliance, financial, reputational, and any other operational risks.
- Support the business to make informed decisions and drive improvements with respect to their control environment.
- Fulfil Treasury's requirement to maintain records and reporting of compliance and risk incidents.
- Provide insight and analysis to the TEB and ARC for management oversight and escalation.
- Assist with incident severity classification and related data to be used to feed Key Risk Indicators as aligned to the Risk Appetite Statement and Risk Management Framework.

Out of Scope

There are separate processes required for instances of fraud, corruption, conflicts of interest, and Workplace Health and Safety (WHS) incidents. For fraud and corruption related incidents refer to the Fraud and Corruption Prevention policy and for WHS related incidents please refer to the WHS Policy. These incidents, however, should still be reported in in Protecht in line with the principles contained in this document.

1.2 Incident Definition

An **incident** is an instance of non-compliance which occurs from non-compliance with:

- an Act or Regulation,
- Treasury internal policies and procedures (TIPPs),
- Treasury issued policies and procedures (TPPs), Directions and Circulars, and
- Relevant Departments' Circulars and Memoranda including of Premier's Department (formerly Department of Premier and Cabinet), Department of Customer Service, and Public Service Commission Circulars.

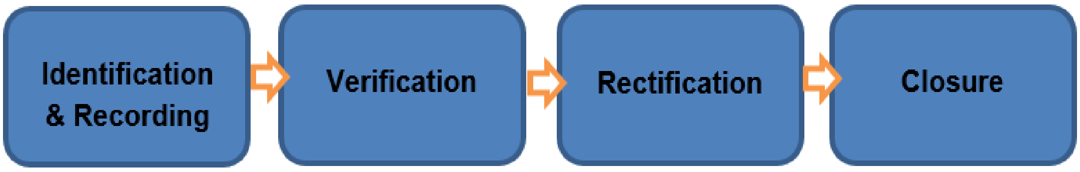
Operational risk incidents and events are also within the scope of this policy. An operational risk event is an event leading to the actual outcome of a business process differing from the expected outcomes, due to inadequate or failed processes or controls, or due to external factors or circumstances. A risk incident is one that has caused, or is likely to cause, a financial, customer or stakeholder, reputational, or regulatory impact to the organisation.

Some examples of compliance and risk incidents are:

- GIPA Act breaches i.e. non-disclosure
- Internal or external fraud i.e. P-Card stolen
- Payment errors
- Approval of expense outside of delegation
- Privacy or Confidentiality breaches
- Data Loss
- Cyber Crime

2 Incident Management Lifecycle

The following steps outline the mandatory process for incident management. More information about these roles and responsibilities are outlined below.



2.1 Identification and Recording

2.1.1 Incident Identification

All employees have a responsibility to identify and report incidents.

Any individual can identify an incident and has the responsibility to notify their Line Manager and to notify the RC&A team. All incidents, irrespective of scale, should be recorded and fall within the scope of this procedure.

All incidents should first be discussed with your manager and then recorded as an entry in the Compliance Breach Incident Register within the risk system Protecht.

More information around the roles and responsibilities of those in bold are set out in **Appendix 1**: Incident Management Roles and Responsibilities.

2.1.2 Incident Classification

Incidents are classified using various criteria according to impact, including, type and severity of compliance breach, potential financial impact, degree of reputational damage, people impact, operational impact, as well as privacy, data and information security impacts.

There are 5 ‘severity’ classifications; Insignificant (1), Minor (2), Moderate (3), Major (4), Extreme (5), which require varying levels of management reporting and escalation. The Incident Classification Matrix (**Appendix 3**) can be used as a guide to classify the severity of each reported incident – this should be used as a guide and professional judgment should be used in cases that do not directly meet certain criteria.

2.1.3 Incident Reporting

It is the responsible of the Line Manager and Director within individual Business Units to log incidents into Protecht. The Treasury RC&A team will liaise and assist internal stakeholders where required to ensure incidents are input into Protecht to meet minimum reporting standards.

Key minimum data with respect to each incident must be captured in standard format. As much information as possible should be provided to enable the nature of the incident to be understood, verified, and assessed.

At a minimum the incident record should contain the following information:

- contact details of incident identifier and incident owner
- date the incident occurred and then was identified
- description of the incident, including the risk impact and potential financial loss, reference to legislation and regulation not complied with, length of non-compliance
- rectification steps undertaken to resolve incident.

Note: All potential losses are to be advised to Treasury Finance Team for provisioning purposes.

If you require any assistance with the kind of information require for this section please reach out to a Risk, Compliance and Audit team member who will be able to assist you.

Once submitted in Protecht, a workflow will be generated for the selected “Incident Owner” for review and confirmation that rectification activities have been completed. Once signed off by the “Incident Owner’, the Director Risk, Compliance and Audit will review to confirm closure.

More information around roles and responsibilities are set out in **Appendix A** (Incident Management Roles and Responsibilities).

See **Appendix B** (Protecht Reporting Input Guidance) for additional information when inputting key fields and data requirements into Protecht.

2.1.4 Data, Privacy, and Confidentiality

In the event of loss of confidential data, privacy issues, or information security breaches, the RC&A team will escalate immediately to the General Counsel and Chief Information Officer to determine the severity classification of the incident, any required regulatory interactions or reporting (eg. to the Information and Privacy Commission) that may be required.

2.2 Verification

For all identified incidents that involve non-compliance with an Act or Regulation, the Director of RC&A will verify that non-compliance has occurred and may seek input from General Counsel to make this determination (based on available information).

The Obligation Owner may assist in determining if non-compliance has occurred and the Director of Audit & Risk will verify this assessment.

2.2.1 Escalation

The nature and timing of escalation is determined by the severity classification of each event. The following escalation criteria should be used to ensure clear, simple, quick, and consistent communication of incidents. The RC&A team will work with each Treasury Business Unit to ensure the below escalation requirements are met:

Severity Classification	E-mail Escalation (notification via employee or RC&A Team as required)	Recording / Input into Protecht (upon advice and confirmation to RC&A team)	Incident Owner
Insignificant (1)	Branch Director & Director Risk, Compliance & Audit	Within 10 working days	Director
Minor (2)	Branch Director & Director Risk, Compliance & Audit	Within 7 working days	Director
Moderate (3)	Branch Director & Director Risk, Compliance & Audit	Within 5 working days	Director
Major (4)	Branch Director & Executive Director & Office of the General Counsel & Director Risk, Compliance & Audit	Within 2 working days	Director
Extreme (5)	Branch Director & Executive Director & Deputy Secretary & Treasury Executive Board (TEB) & Office of the General Counsel & Director Risk, Compliance & Audit	Within 24 hours	Executive Director

2.3 Rectification and Remediation

The incident owner is accountable for overseeing the completion of rectification activities for the incident, which should be documented within Protecht.

An integral component of the incident rectification process is the identification of the cause of the incident and the subsequent adoption of controls to mitigate a future recurrence. New controls could include:

- process or system improvements
- changes to procedures
- additional checks and reviews
- education and awareness training
- a manual work-around in the absence of an immediate long term fix.

In some cases, public-facing, intra-agency, or regulatory remediation may be required; this could include instances of incident correspondence (confirmation, actions for closure, resolution, etc) with a regulatory body or members of the public. These should be clearly investigated and documented where required. Individual Business Units should liaise with General Counsel and the RC&A team where required to document and track status.

2.4 Closure

The incident owner is to inform the RC&A team of the closure of the incident, once the following steps have been completed:

- All known impacts relating to the event have occurred, been captured and validated
- No further impacts are reasonably foreseen with the creation of new or improved controls
- all rectification activities are complete, and there are no outstanding items
- the correct “actual” financial loss has been advised and recorded on Protecht if applicable
- if required, a risk acceptance to be submitted via Protecht to risk accept before closure.

The RC&A Team will review the incident and will close the incident in Protecht when all rectification steps have been completed.

There may be instances when an incident can be reopened, if there is evidence to indicate the remediation steps maybe not be sufficient. In these cases the RC&A team will notify the relevant business units.

3 Risk and Compliance Management Reporting

3.1 Reporting

The Director of RC&A is responsible for reporting compliance incidents, depending on the nature and materiality based on incident severity classification. Incidents will be reported to the Treasury Executive Board (TEB) in line with escalation requirements and Treasury’s Audit & Risk Committee (ARC) on a quarterly basis.

Incident data will be analysed and reported to the ARC to assist with the identification of trends, control failures, systemic issues or other additional issues requiring corrective action.

Incident data will also be used to inform other elements of the Compliance Management Framework, the Risk Management Framework, and the Risk Appetite Statement, including Risk and Compliance Obligation Workshops, and Key Risk Indicators.

4 Protocols of Engagement

RC&A will engage with various incident owners and their direct reports, senior management, and the Audit and Risk Committee (ARC) using the following guidelines:

- As incidents are identified; to consult and confirm with the RC&A team
- The RC&A team consult and assist Business Units with the timely input of incidents into Protecht
- The RC&A team to own escalation notification activities as detailed in **Appendix B**

- Business Units to provide monthly status updates relating to rectification activities. The RC&A team will document updates in Protecht and track for closure in line with estimated timelines. Incident status updates will be used as a part of quarterly ARC reporting.

Related Policies and Documents

Issuer	Reference	Document Name
Director RC&A	TIPP5.01	Risk Management Framework
Director RC&A	TIPP5.09 & TIPP5.10	Fraud and Corruption Control Plan Fraud and Corruption Control Framework
International Standards Organisation	ISO 31000:2018 & ISO 37301:2021	Risk Management – Guidelines & Compliance Management Systems – Guidelines
NSW Government	[No 17 of 1998]	State Records Act 1998 No 17
Secretary	TIPP2.05	Code of Ethics and Conduct
NSW Treasury (Financial Management Legislation, Policy & Assurance branch)	TPP20-08	Internal Audit and Risk Management Policy for the General Government Sector (TPP20-08)
General Counsel	TIPP5.04	Public Interest disclosures Internal reporting policy

Appendix A: Incident Management Roles and Responsibilities

Role	Responsibility
Incident Identifier Can be any member of staff or external stakeholder (i.e. The Audit Office)	Report an incident via Treasury's risk system Protecht in a timely manner sharing as much detail as possible, including if applicable, the potential financial loss.
Incident Owner Director or above (the owner may also be the identifier)	Co-ordinate the development and execution of a rectification plan in conjunction with relevant stakeholders. ▪ Prepare status reports and the final report as required ▪ Ensure that an accurate record has been created by the Incident Identifier within Protecht ▪ Ensure that the incident is rectified in a timely manner ▪ If required, provide additional information for reporting purposes.
Obligation Owner	Assigned owner of a compliance obligation as set out in the Treasury Compliance Obligations Register.
Director of RC&A	▪ Ensure that all identified incidents are recorded accurately and completely in Protecht ▪ Provide advice on impact and associated risk and control failures ▪ Review and approve incidents in Protecht when signed off by incident owner.
General Counsel	▪ Provide technical legal advice as required. ▪ Privacy Officer to liaise with incident owners and the RC&A team to complete a Privacy / Data Breach form as required.
Branch Executive Director	▪ Responsible for the overall management and reporting of incidents from their branch. ▪ Ensure that all identified incidents from their division are recorded accurately and completely in Protecht.

Appendix B: Protecht Reporting Input Guidance (Key fields)

Protecht Field	Additional Information
Incident Type	Fraud, General Compliance, or Other.
Identified By	The name of the Treasury Staff who identified or raised the incident.
Group / Division Identified By	The team name of the Treasury Staff who identified or raised the incident.
If reported by External Agency - Agency Name	In some cases the incident may have been reported by an external stakeholder.
Incident Owner	The name of the Treasury Staff who will own the incident and who will ultimately sign off once all rectification, remediation, and closure activities have been completed. The Incident Owner will often be responsible for the controls or obligations in relation to the root cause deficiency or failure as documented in the 'Incident Detail' field. The Incident Owner will co-ordinate the development and execution of a rectification plan in conjunction with relevant stakeholders. In some rare cases there can be joint ownership assigned to an incident.
Group / Division Owned By	The team name of the Treasury staff member who owns the incident.
Incident Title	A detailed and succinct summary of the incident.
Incident Detail	This field should include detailed of the incident including root cause analysis and investigation and understanding of failed controls. A clear description of the event and the resulting effects. Detail any specific lesson(s) that have been learnt as a result of this incident to prevent recurrence.
How was the Incident Discovered	A clear description of how the incident was discovered – i.e. through internal review / investigation / audit, a complaint, notification from a regulator, etc.

Appendix C: Incident Classification Matrix

Severity Classificatio n	Potential Financial Impact ($)	Reputational Impact	Confidentiality Breach / Information Security / Data Protection / Privacy – number of stakeholders impacted. (i.e. members of NSW Public, Supplier, Other Agency, etc)	Compliance Impact including: Regulatory, Legislative, Treasury internal policies and procedures (TIPPs); Treasury issued policies and procedures (TPPs), Directions and Circulars; Relevant Department Circulars and Memoranda	Process / Business Operations Impact
Insignificant (1)	< | 25,000 |	Low level of local / regional media coverage.	Internal Data Breach < 20 internal staff affected. The breach has been rectified within 24 hours and there is no notification required to the Privacy Commissioner.	- Negligible non-compliance with minimal impact on operational business processes. - Rare legislative non-compliance, little or no effect on business operations. - Negligible impact on local environment.	- Small deviation from an Operational Process.
Minor (2)	| 25,000 | - | 50,000 |	Local / Regional or National media coverage.	Data Breach between NSW government agencies. < 20 stakeholders / parties affected. The breach has been rectified within 24 hours and there is no notification required to the Privacy Commissioner.	- Regulatory non-compliance requiring local staff effort to rectify. - Isolated legislative non-compliance, effect managed at operational level. - Minimal impact on local environment.	- Some delays and/or minor impact on Operational Process. - Limited IT system / applications / operational process delay or outage (<1/2 day)
Moderate (3)	| 50,000 | - | 100,000 |	Sustained National media coverage.	External Data Breach – data has left or unintentionally sent or lost from Treasury secured network. < 20 stakeholders / parties affected. Where after the privacy breach assessment has been undertaken and the matter results in no or minimal damage to the individuals concerned – depending on the level of breach, a Notification of Data Breach would have to be sent to the IPC.	- Regulatory non-compliance requiring management effort to rectify and / or limited notification to a regulatory authority. - Control failures resulting in frequent legislative non-compliance. - Significant effect on Treasury business operations requiring changes to business processes. - Some impact on local environment	- Some delays and/or minor impact on Operational Process. - Limited IT system / applications / operational process delay or outage (<1 day)
Major (4)	| 100,000 | - | 250,000 |	International Media coverage / Government Investigation / Parliamentary Hearing.	External Data Breach – data has left or unintentionally sent, lost, or stolen from Treasury secured network. > 20 stakeholders / parties affected by the inadvertent disclosure of highly sensitive information. Privacy Commissioner is notified of the Breach and remedial action is required	- Regulatory non-compliance resulting in notification by a regulatory authority. - Grossly negligent breach of legislation. - Formal investigations, disciplinary action, ministerial involvement. - Substantial impact on local and surrounding environments.	- Numerous defects on a system or operational process. - Core system / applications / operational process delay or outage (<1 day)
Extreme (5)	> | 250,000 |	Sustained International Media coverage / Fines or Sanctions / Prosecutions / Dismissals.	External Data Breach – data has left or unintentionally sent, lost, or stolen from Treasury secured network. > systemic issue affecting many parties / stakeholders affected by the inadvertent disclosure of highly sensitive information. Incident identifies a major deficiency in the Information Security / Confidentiality / Privacy control environment. Privacy Commissioner is notified of the breach, and significant remedial action is required.	- Significant non-compliance which may result in fine to agency and/or prosecution. - Widespread serious or wilful breach. - Prosecutions, dismissals and Parliamentary scrutiny. - Severe impact on local and surrounding environments.	- Numerous defects on core systems and key operational processes. - Core system / applications / operational process delay or outage (<1 day).

52 Martin Place
Sydney NSW 2000

GPO Box 5469
Sydney NSW 2001

W: treasury.nsw.gov.au