From: s47F(1)
To: s47F(1)
Cc: s47F(1) s47F(1) ; s47F(1) ; s47F(1) ; s47E(d) s47F(1)
Subject: RE: s47E(d) [SEC=OFFICIAL:Sensitive]
Date: Friday, 12 December 2025 10:18:00 AM

Good morning, s47F(1)
Thank you for your email, I will review and provide any comments requiring clarification, I will reach out to you early next week.
I will review the draft report and progress through to Sally once we both are comfortable.
Just to clarify, you have sent this draft report from your KPMG email, have you prepared this draft report outside of the SA network?
Kind regards
s47F(1)

From: s47F(1)
Sent: Friday, 12 December 2025 9:20 AM
To: s47F(1) ; s47E(d)
Cc: s47F(1) ; s47F(1) ; s47F(1)
Subject: s47E(d)

Caution: Do not click any links or open any attachments unless you trust the sender and believe the content to be safe.

Good morning s47F(1) ,
Please see attached the Draft Report for the s47E(d) review.
As discussed, the work conducted covered s47E(d)
We have added
that extra context throughout the report.
s47E(d)
s47E(d)

Secondly, I was hoping you would have the date
for when the s47E(d) occurred for inclusion of
Appendix A, I unfortunately do not have that email on my Services account.

Please reach out to myself or the team if you have any questions,
Kind regards
s47F(1)
s47F(1)

KPMG
s47F(1)

s47F(1) @kpmg.com.au
u

****

©2025 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation. Liability limited by a scheme approved under Professional Standards Legislation.

****

From: s47F(1)
To: Bond, Sally
Subject: KPMG issue for discussion [SEC=OFFICIAL]
Date: Wednesday, 17 December 2025 4:22:00 PM
Attachments: KPMG - business case.docx
image001.png
Importance: High

Hi Sally,

While I was off, the team picked up an issue where it appears KPMG has taken agency materials outside of the network which is in breach of their obligations under the contract. s47F(1) has summarised the issue in the word document attached. The specific instance related to the s47E(d) report being sent from an external KPMG email address.

We'll discuss this with you tomorrow at the audit delivery catchup.

I'll propose we take a few steps here:

1. Remind KPMG of their obligations
2. Request KPMG:
    a. identify and report back on all materials taken outside of the agency networks
    b. provide an explanation on how the materials were taken outside the network (to identify the control gap issues)
    c. remove any agency material taken outside of the agency networks
    d. provide assurance that all materials taken outside have been deleted/destroyed and there are no uncontrolled versions

Once we have that information, we can then assess whether any further action is required (including termination of contracts, noting there is no remedy available for a breach of this nature) and who else needs to be informed.

Thanks

s47F(1)
s47F(1) **Director**
Audit Branch
Corporate and Cross Government Services Division
s47F(1)

Services Australia acknowledges the Traditional Custodians of the lands we live on. We pay our respects to all Elders, past and present, of all Aboriginal and Torres Strait Islander nations.

From: s47F(1)
Sent: Tuesday, 16 December 2025 6:16 PM
To: s47F(1)
Subject: Business case -KPMG [SEC=OFFICIAL]

Hi s47F(1)

As we discussed, please find attached a summary for KPMG's matter.

Please also find attached the respective communications and other references.

Thank you and kind regards,
s47F(1)

1. On Friday,12 December 2025 at 9.20am, s47F(1) (KPMG's specified personnel to deliver audit activities for the Agency) sent the s47E(d) (marked as OFFICIAL: Sensitive) from his KPMG's mailbox s47F(1) @kpmg.com.au) to the SA's audit manager s47F(1) email s22 @servicesaustralia.gov.au) and s47E(d) mailbox. The email was CCed to s47F(1) SA' mailbox s47F(1) @servicesaustralia.gov.au) and also allegedly distributed outside of the SA's network by sending a copy of the report via CCing it to s47F(1) ' KPMG mailbox s47F(1) @kpmg.com.au) and s47F(1) KPMG mailbox s47F(1) @kpmg.com.au).
2. Soon after (at10.19 am on the same day), s47F(1) (the audit manager) replied to s47F(1) email to clarify if the draft audit report was prepared outside of the SA network.
3. s47F(1) did not answer the above question and did not reply to s47F(1) email.
4. Instead, a separate email was sent at 10.44 am from s47F(1) SA's mailbox (s47F(1) @servicesaustralia.gov.au) with the link to the report at SharePoint site s47E(d) to be reviewed.
5. For note, it is unknown when and by whom the draft report for s47E(d) audit and possibly any other agency's information was sent outside SA's network.
6. To appropriately manage the agency information within SA's network, the KPMG's personnel were provided with access to a dedicated to Service Provider shared folder and other SA's facilities, such as an established for the auditor's TEAMS's group and a SharePoint site.
7. s47E(d), s47G

   the MAS Panel Head Agreement, s47E(d), s47G the following clauses:

   - The Agency Material Clause (refer to page 5):
     "The Service Provider must not, and must ensure that its Personnel (including the Personnel of its Subcontractors) do not:
     (a) remove Agency Material or allow Agency Material to be removed from Agency Property or premises (whether in digital or physical form)",
     and
     "The Service Provider acknowledges that Agency Material acquired by it is not to be disclosed, published or communicated to any unauthorised person in any form either during or after the Contract Term."
   - The Agency Security Clause (refer to page 6):
     "The Service Provider acknowledges that Services Australia must comply with the Australian Government Protective Security Policy Framework ('PSPF'). The Service Provider must, and must ensure that its Personnel and subcontractors comply with:

(a) all relevant requirements of the PSPF, including the plans and protocols of Services Australia, in its application to Personnel, information and asset security."

- Confidential Information Clause (refer to page 6):

Agency Confidential information	Period of Confidentiality
Agency data	*Indefinitely*
Any Personal Information held by the Agency	Indefinitely
Security Classified Information	*Indefinitely*

8. s47E(d)

- Clause 7.12 (b): "*the Service Provider must ensure that its personnel comply with the Service Provider's obligation in this head Agreement and any Contract*."
- Clause 20.1.3: "*the Service Provider agrees to ensure Agency materials is used strictly in accordance with any conditions or restrictions specified in an order and any direction from the Agency*."
- Clause 23.1.1: "*the Service Provider agrees to comply with any applicable security requirements specified in the Protective Security Policy Framework (including those provisions relevant to Commonwealth contracted service providers), as required by an Agency in an Order*."

9. As a consequence, the agency may terminate the contract for default under clause 26.2.1: "*If the Service Provider fails to satisfy any of its obligations under a Contract, and the Agency considers that the failure is (a) not capable of remedy,* the Agency may, by notice terminate the Contract immediately".
10. Furthermore, the agency may terminate or reduce the services under the Contract for convenience under clause 26.4.1: "the *agency may by 10 Business Days' note, at any time and in its absolute discretion terminate a Contract or reduce the scope of any Ordered Service*."
11. In addition to the above, the Service Provider must comply with the Data Security obligations under the Deed and *"must immediately notify Finance and any relevant Agency if there is a Security Incident or a breach of any of the Service Provider's obligations under this clause 23, by the Service Provider or any of its Personnel or Subcontractors*."

From: s47F(1)
To: s47F(1) Bond, Sally
Cc: s47F(1) ; s47F(1)
Subject: RE: KPMG information security incident [SEC=OFFICIAL]
Date: Tuesday, 23 December 2025 8:36:00 AM
Attachments: image001.png
image002.png

Hi Sally

Nothing to add.

Thank you, s47F(1)

From: s47F(1)
Sent: Tuesday, 23 December 2025 8:34 AM
To: Bond, Sally
Cc: s47F(1) ; s47F(1) ; s47F(1)
Subject: RE: KPMG information security incident [SEC=OFFICIAL]

Hi Sally,

Happy for it to go as is.

Thanks

s47F(1)

From: Bond, Sally s47F(s47F(1)@servicesaustralia.gov.au>
Sent: Tuesday, 23 December 2025 8:01 AM
To: s47F(1) @servicesaustralia.gov.au>
Cc: s47F(1) @servicesaustralia.gov.au>; s47F(1) @servicesaustralia.gov.au>; s47F(1) @servicesaustralia.gov.au>
Subject: RE: KPMG information security incident [SEC=OFFICIAL]

Hi s47F(1) ,

Apologies, this email slipped through the cracks and I will get out today. I will give them until 8 Jan to respond.

I just wanted to check if there is any update or if it needs to be changed in anyway before I send.

Thank you!

Sally

From: s47F(1) @servicesaustralia.gov.au>
Sent: Thursday, 18 December 2025 2:52 PM
To: Bond, Sally s47F(1) @servicesaustralia.gov.au>
Cc: s47F(1) @servicesaustralia.gov.au>; s47F(1) @servicesaustralia.gov.au>; s47F(1) @servicesaustralia.gov.au>
Subject: KPMG information security incident [SEC=OFFICIAL]

Hi Sally,

As discussed at the Audit Delivery catchup, please see below a draft email to be sent to KPMG outlining the issue, reminding them of their obligations, and requesting action.

The date for return of the information has been left in yellow highlight. Potentially we

ask for a return by 2 January?

I've asked s47F(1) to commence the process internally, and lodge the incident via the following channels. We can update the report as more information comes to hand (including lodging a privacy incident if it is identified through our enquiries that it is required.

Report a Security Incident

Report a Cyber Security incident

Security Branch are the information security policy owners. I've reached out to s47F(1) s47F(1) for some advice, and will update when I hear back.

Thanks

s47F(1)

----DRAFT EMAIL----------

To: s47F(1) @kpmg.com.au

Cc: s47F(1) @servicesaustralia.gov.au; s47F(1) @servicesaustralia.gov.au; s47E(d) @servicesaustralia.gov.au; s47E(d) @servicesaustralia.gov.au

Subject: FOR RESPONSE BY XXX: Audit information outside of agency systems

s47C

From: Bond, Sally
To: s47F(@kpmg.com.au; Bond, Sally
Cc: s22 ; s22 ; s22 ; s47E(d) ; s47E(d) ; s47E(d)
Subject: FOR IMMEDIATE ACTION: KPMG information security incident [SEC=OFFICIAL]
Date: Tuesday, 23 December 2025 9:39:00 AM
Attachments: image002.png
Importance: High

---

s47F(1)

FOR ACTION BY TUESDAY 6 JANUARY 2026: KPMG INFORMATION SECURITY INCIDENT

We very recently became aware that information was transferred outside of the Services Australia environment by KPMG during our engagement in relation to the s47E(d) internal audit. This was detected when the draft report was provided from a KPMG email address rather than the assigned Services Australia email address. A brief summary of events is included below:

- On Friday 12 December 2025 at 9.20am, s47F(1) (KPMG's specified personnel to deliver audit activities for the agency) sent the draft report for s47E(d) (marked as OFFICIAL: Sensitive) from his KPMG's mailbox s47F(1) @kpmg.com.au) to the agency's audit manager s47F(1) email (s47F(1) @servicesaustralia.gov.au) and the s47E(d) mailbox. The email was CC'ed to s47F(1) s47F(1) @servicesaustralia.gov.au) and also s47F(1) KPMG mailbox (s47F(1) @kpmg.com.au) and s47F(1) KPMG mailbox s47F(1) @kpmg.com.au).
- Soon after (at 10.19 am on the same day), s47F(1) replied to s47F(1) email to clarify if the draft audit report was prepared outside of the SA network.
- Subsequent discussions between s47F(1) and s47F(1) have occurred, confirming information is held by KPMG outside of the Services Australia environment.

Removing information outside of the Services Australia environment presents privileged information, privacy, confidentiality and security risks, and is explicitly prohibited under the contract. Specifically, the following clauses, amongst others from the Order for Services (D40804098, Schedule 6 under the MAS Panel Head Agreement, executed on 3 April 2025) outline the expectations:

- The Agency Material Clause (refer to page 5):

  "The Service Provider must not, and must ensure that its Personnel (including the Personnel of its Subcontractors) do not:

  a. *remove Agency Material or allow Agency Material to be removed from Agency Property or premises (whether in digital or physical form)",*

  and

  "The Service Provider acknowledges that Agency Material acquired by it is not to be disclosed, published or communicated to any unauthorised person in any form either during or after the Contract Term."

- The Agency Security Clause (refer to page 6):

  "The Service Provider acknowledges that Services Australia must comply with the Australian Government Protective Security Policy Framework ('PSPF').

  The Service Provider must, and must ensure that its Personnel and

subcontractors comply with:

(a) all relevant requirements of the PSPF, including the plans and protocols of Services Australia, in its application to Personnel, information and asset security."

- Confidential Information Clause (refer to page 6):

Agency Confidential information	Period of Confidentiality
Agency data	*Indefinitely*
Any Personal Information held by the Agency	Indefinitely
Security Classified Information	*Indefinitely*

The MAS Panel Head Agreement also requires:

- Clause 7.12 (b): "*the Service Provider must ensure that its personnel comply with the Service Provider's obligation in this head Agreement and any Contract*."
- Clause 20.1.3: "*the Service Provider agrees to ensure Agency materials is used strictly in accordance with any conditions or restrictions specified in an order and any direction from the Agency*."
- Clause 23.1.1: "*the Service Provider agrees to comply with any applicable security requirements specified in the Protective Security Policy Framework (including those provisions relevant to Commonwealth contracted service providers), as required by an Agency in an Order*."

Additionally, depending on the nature of the information transferred, KPMG has obligations to "*immediately notify Finance and any relevant Agency if there is a Security Incident or a breach of any of the Service Provider's obligations under this clause 23, by the Service Provider or any of its Personnel or Subcontractors*."

IMMEDIATE ACTIONS REQUIRED

We require KPMG to undertake a review of its handling of agency materials as it relates to each of the following four engagements and take steps to remove and delete information outside of the agency's networks:

- s47E(d)
- s47E(d)
- s47E(d)
- s47E(d)

Noting time is of the essence, please provide a written response, by **Tuesday 6 January 2026** to s47F(1) @servicesaustralia.gov.au containing:

- A listing of all agency materials KPMG has transferred outside of the Services Australia environment (including via email, MS Teams, file transfer or any other methods) through the above engagements.
- A detailed explanation as to how the materials were taken outside the Services Australia environment including those personnel directly involved and those personnel who were aware of the breach.

- Details of any internal KPMG investigations undertaken as a result of this breach including reporting to internal and external parties.
- Assurance that all materials taken the Services Australia environment have been deleted/destroyed, and there are no uncontrolled versions in existence.

Services Australia takes a breach of this nature extremely seriously. We will be in parallel engaging with our relevant agency teams to undertake a review of the situation. We will advise any further steps once we have a more complete picture of the situation.

Kind regards

Sally

Sally Bond
National Manager, Audit
Audit Branch, Corporate and Cross Government Services Division
s47F(1)



s47F(1)

Services Australia acknowledges the Traditional Custodians of the lands we live on. We pay our respects to all Elders, past and present, of all Aboriginal and Torres Strait Islander nations.

From: Bond, Sally
To: Blair, Teresa
Subject: FW: FOR IMMEDIATE ACTION: KPMG information security incident [SEC=OFFICIAL]
Date: Tuesday, 23 December 2025 9:42:00 AM
Attachments: image002.png
Importance: High

Hi Teresa,
Just giving you a heads up on this one.
The audit branch has identified a security breach involving KPMG. It has been identified that KPMG has taken information outside the Services Australia environment which is a breach of our contract with them.
I was only made aware of this late last week. My team has engaged with the security branch to determine next steps.
I have sent the below email to KPMG today to ask for a formal explanation.
I do not believe that the information, that we are currently aware of, that has been taken is of particular concern. I am more concerned that KPMG has acted outside the contract and has not taken any proactive steps to assure us of this fact.
Happy to chat, otherwise we will chat in the new year.
Sally

From: Bond, Sally
Sent: Tuesday, 23 December 2025 9:39 AM
To: s47F(1) @kpmg.com.au' ; Bond, Sally
Cc: s22 ; s22 ; s47F(1) ; s47E(d) ; s47E(d) ; s47E(d)
Subject: FOR IMMEDIATE ACTION: KPMG information security incident [SEC=OFFICIAL]
Importance: High

s22 (duplicate information)

From: s47F(1)
To: Bond, Sally
Subject: RE: FOR IMMEDIATE ACTION: KPMG information security incident [SEC=OFFICIAL]
Date: Tuesday, 23 December 2025 10:28:09 AM
Attachments: image002.jpg
image003.jpg
image004.jpg
image005.jpg
image006.jpg
image007.png

Caution: Do not click any links or open any attachments unless you trust the sender and believe the content to be safe.

Hi Sally,

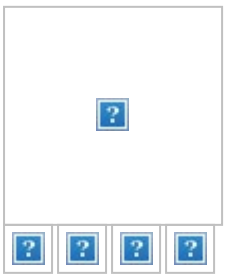
I believe that s47F(1) will reach to you.

Thanks

s47F(1)

s47F(1)
Executive Assistant to s47F(1) , s47F(1) and s47F(1)
Consulting
s47F(1)
s47F(1) @kpmg.com.au

I'm sending this message now because the timing works for me, and I don't expect that you will read, respond to or action it outside of your regular working hours.



I acknowledge Aboriginal and Torres Strait Islander peoples as the Traditional Custodians of the land on which I live and work.

From: Bond, Sally
Sent: Tuesday, 23 December 2025 9:57 AM
To: s47F(1)
Subject: [EXTERNAL] FW: FOR IMMEDIATE ACTION: KPMG information security incident [SEC=OFFICIAL]

CAUTION: This Email is from an EXTERNAL source. Ensure you trust this sender before clicking on any links or attachments.

Hi s47F(1)

I have sent s47F(1) a very important email this morning that needs immediate action. Could you please advise ASAP who I should contact in s47F(1) absence? The matter involves a breach of security by KPMG and cannot wait until his return.

Sally
Sally Bond
National Manager, Audit

Audit Branch, Corporate and Cross Government Services Division
s47F(1)



s47F(1)
Services Australia acknowledges the Traditional Custodians of the lands we live on. We pay our respects to all Elders, past and present, of all Aboriginal and Torres Strait Islander nations.

From: s47E(d) @kpmg.com.au>
Sent: Tuesday, 23 December 2025 9:40 AM
To: Bond, Sally s47F(1) @servicesaustralia.gov.au>
Subject: Automatic reply: FOR IMMEDIATE ACTION: KPMG information security incident [SEC=OFFICIAL]

Caution: Do not click any links or open any attachments unless you trust the sender and believe the content to be safe.

Thank you for your email. s47F(1) For urgent requests please contact my EA s47F(1) on s47F(1) @kpmg.com.au. Regards s47F(1)
****

The information in this e-mail is confidential and may be legally privileged. It is intended solely for the addressee. Access to this e-mail by anyone else is unauthorized. If you have received this communication in error, please address with the subject heading "Received in error," send to the original sender , then delete the e-mail and destroy any copies of it. If you are not the intended recipient, any disclosure, copying, distribution or any action taken or omitted to be taken in reliance on it, is prohibited and may be unlawful. Any opinions or advice contained in this e-mail are subject to the terms and conditions expressed in the governing KPMG client engagement letter. Opinions, conclusions and other information in this e-mail and any attachments that do not relate to the official business of the member firm are neither given nor endorsed by it.

KPMG cannot guarantee that e-mail communications are secure or error-free, as information could be intercepted, corrupted, amended, lost, destroyed, arrive late or incomplete, or contain viruses.

This email is being sent out by KPMG International on behalf of the local KPMG member firm providing services to you. KPMG International Limited is a private English company limited by guarantee. KPMG International Limited and its related entities do not provide services to clients. Each KPMG firm is a legally distinct and separate entity and describes itself as such. Each KPMG member firm is responsible for its own obligations and liabilities.
For more detail about our structure please visit home.kpmg/governance.

This footnote also confirms that this e-mail message has been swept by AntiVirus

software.

****

****

IMPORTANT: This e-mail is for the use of the intended recipient only and may contain information that is confidential, commercially valuable and/or subject to legal or parliamentary privilege. If you are not the intended recipient you are notified that any review, re-transmission, disclosure, dissemination or other use of, or taking of any action in reliance upon, this information is prohibited and may result in severe penalties. If you have received this e-mail in error please notify the sender immediately and delete all electronic and hard copies of this transmission together with any attachments. Please consider the environment before printing this e-mail

****

****

©2025 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation. Liability limited by a scheme approved under Professional Standards Legislation.

****

From: s47F(1)
To: Bond, Sally
Cc: s47F(1) ; s47F(1) ; s47F(1) ; s47F(1) ; s47F(1) ; s47E(d) ; s47E(d) s47E(d)
Subject: RE: FOR IMMEDIATE ACTION: KPMG information security incident [SEC=OFFICIAL]
Date: Tuesday, 23 December 2025 2:36:01 PM
Attachments: image001.png

Caution: Do not click any links or open any attachments unless you trust the sender and believe the content to be safe.

Hi Sally
Per our quick chat earlier, I'm responding on behalf of s47F(1) as he is currently on leave.
I can confirm from our investigation that the only document transferred out of the Services Australia network was the Internal Audit Report Template. s47F(1) then used this template to draft the report, which was then sent from his KPMG email account.
s47F(1) and s47F(1) we cc'd on this email and I can confirm that they have deleted this email and that no uncontrolled versions are in existence.
s47F(1) has spoken to all KPMG staff working on Internal Audit work for Services Australia and reiterated security requirements and the importance of no Services Australia documents leaving the Services Australia network. s47F(1) has been spoken to directly on this matter and will undergo follow up actions, including additional training, in the new year.
Regards,
s47F(1)

From: Bond, Sally s47F(1) @servicesaustralia.gov.au>
Sent: Tuesday, December 23, 2025 9:39:15 AM
To: s47F(1) s47F(1) @kpmg.com.au>; Bond, Sally s47F(1) @servicesaustralia.gov.au>
Cc: s47F(1) @servicesaustralia.gov.au>; s47F(1) @servicesaustralia.gov.au>; Bond, Sally s47F(1) @servicesaustralia.gov.au>; s47E(d) @servicesaustralia.gov.au>; s47E(d) @servicesaustralia.gov.au>; s47E(d) @servicesaustralia.gov.au>
Subject: [EXTERNAL] FOR IMMEDIATE ACTION: KPMG information security incident [SEC=OFFICIAL]

s22 (duplicate information)

From: s47F(1)
To: Bond, Sally
Subject: FW: s47E(d) SA information sent outside of the agency"s network/system. [SEC=OFFICIAL]
Date: Friday, 2 January 2026 4:13:46 PM
Attachments: image001.png
image003.png
image004.png
image005.jpg

Hi Sally
FYI
Kind regards
s47F(1)

From: s47E(d)
Sent: Friday, 2 January 2026 12:25 PM
To: s47F(1) ;s47E(d)
Cc: s47F(1) ;s47F(1) ;s47E(d) ;s47E(d)
Subject: RE: s47E(d) - SA information sent outside of the agency's network/system. [SEC=OFFICIAL]
Good afternoon s47F(1)
Based on the Security Markings page available on the intranet, I do not believe there are specific limits on files labelled OFFICIAL : Sensitive being sent outside of the network if going towards contractors engaged for the work. The content is work relevant and the file is appropriately classified. The user has access to a Services Australia account so they could simply email themselves the draft copy for editing, if the email was appropriately classified again I don't see wrongdoing from a cyber perspective.
Regarding the second email, users outside of our tenancy will not be able to access our internal sharepoint due to cyber policy, people cc'd in the email will need a SA account before they will be able to access the content.
The above is based on a reading of the policy page and is simply my interpretation of the guidelines. Security classification/data loss prevention is beyond the scope of cyber operations so if you want a definitive answer consider reaching out to s47E(d) @servicesaustralia.gov.au.
Kind regards,
s47F(1)
s47F(1)
Cyber Operations / Cyber Services Division

I acknowledge the Traditional Custodians of the lands we live on. I pay my respects to all Elders, past and present, of all Aboriginal and Torres Strait Islander nations.

From: s47F(1) @servicesaustralia.gov.au>
Sent: Friday, 2 January 2026 11:52 AM
To: s47E(d) @servicesaustralia.gov.au>
Cc: s47F(1) @servicesaustralia.gov.au>;s47F(1) @servicesaustralia.gov.au>
Subject: RE s47E(d) - SA information sent outside of the agency's network/system. [SEC=OFFICIAL]
Good morning
Thank you very much for your email.
The reason I raised this cyber incident because I received the email from s47F(1) @kpmg.com.au (external user) on 12 December 2025 9:21:49 12 December 2025 9:21:49 AM with an attachment classified as **OFFICIAL:Sensitive**. This email included two additional external recipients s47F(1) @kpmg.com.au and s47F(1) @kpmg.com.au).

[PDF copies of all three emails are available in the incident report]

Question is how the user was able to remove a file from the SA network with OFFICIAL:Sensitive classification without tripping any system controls to send it back?
When I asked the question if the document was prepared outside of the SA network, the user provided a separate email from their internal (SA) email with the SharePoint link.
The email containing a SharePoint link (mentioned below) was sent from an internal email s47F(1) @servicesaustralia.gov.au), there was no issue with this email. It was a secondary reply by the user.

Please feel free to contact me if needed.
Kind regards
s47F(1)
s47F(1)
Phone: s47F(1) | Mobile: s47F(1)
Audit Branch | CCGS
s47F(1)

Services Australia acknowledges the Traditional Custodians of the lands we live on. We pay our respects to all Elders, past and present, of all Aboriginal and Torres Strait Islander nations.

s47E(d) **@servicesaustralia.gov.au**

From: s47E(d) @servicesaustralia.gov.au>
Sent: Wednesday, 24 December 2025 6:09 AM
To: s47F(1) @servicesaustralia.gov.au>
Cc: s47F(1) @servicesaustralia.gov.au>; s47E(d) @servicesaustralia.gov.au>
Subject: s47E(d) - SA information sent outside of the agency's network/system. [SEC=OFFICIAL]

Good morning s47F(1)
Thank you for reporting the incident. The link on the email assessed to be an Internal SharePoint link which it is not accessible by external businesses. Hence Cyber risk and the possibility of the Data Breach assessed to be low at this stage.
Also, FYI, this incident is not a Cyber Security incident. For further information on Eligible Data Breaches please send an email to s47E(d) @servicesaustralia.gov.au and complete the Report a Privacy Incident.

Kind Regards,
s47F(1)
Cyber Security Operation Branch
Cyber Security Division
s47F(1)
s47F(1)

From: s47F(1)
To: s47E(d)
Subject: FW: s47E(d) - SA information sent outside of the agency"s network/system. [SEC=OFFICIAL]
Date: Wednesday, 7 January 2026 11:29:00 AM
Attachments: image001.png
image003.png
image004.png
image005.jpg

Hi s47F(1

FYI - as discussed.

Kind regards

s47F(1)

From s47E(d)
Sent: Friday, 2 January 2026 12:25 PM
To: s47F(1) ;s47E(d)
Cc: s47F(1) ;s47F(1) ;s47E(d) ;s47E(d)
Subject: RE: s47E(d) - SA information sent outside of the agency's network/system. [SEC=OFFICIAL]

s22 (duplicate information)

From: s47F(1) @servicesaustralia.gov.au>
Sent: Friday, 2 January 2026 11:52 AM
To: s47E(d) @servicesaustralia.gov.au>
Cc: s47F(1) @servicesaustralia.gov.au>;s47F(1) @servicesaustralia.gov.au>
Subject: RE: s47E(d) - SA information sent outside of the agency's network/system. [SEC=OFFICIAL]

s22 (duplicate information)

s22 (duplicate information)

From: s47E(d) @servicesaustralia.gov.au>
Sent: Wednesday, 24 December 2025 6:09 AM
To: s47F(1) @servicesaustralia.gov.au>
Cc: s47F(1) @servicesaustralia.gov.au>; s47E(d) @servicesaustralia.gov.au>
Subject: s47F(d) - SA information sent outside of the agency's network/system. [SEC=OFFICIAL]

s22 (duplicate information)

From: Bond, Sally
To: Blair, Teresa
Cc: s47E(d) s47E(d)
Subject: FW: FOR IMMEDIATE ACTION: KPMG information security incident [SEC=OFFICIAL]
Date: Tuesday, 6 January 2026 4:14:00 PM
Attachments: image001.png

Hi Teresa,
As discussed, please see the response from KPMG below.
If you send a reply, the two key people to reply to are:

- s47F(1) @kpmg.com.au
- s47F(1) @kpmg.com.au

We have looked at the contract, which is the standard MAS contract from the Dept of Finance, and there are no clauses relating to breach of the terms of the contract or penalties etc.
Please reach out if you have any questions.

Sally

From: s47F(1)
Sent: Tuesday, 23 December 2025 2:30 PM
To: Bond, Sally
Cc: s47F(1) ; s47F(1) ; s47F(1) ; s47F(1) ; s47F(1) ; s47E(d) ; s47E(d) ; s47E(d)
Subject: RE: FOR IMMEDIATE ACTION: KPMG information security incident [SEC=OFFICIAL]

Caution: Do not click any links or open any attachments unless you trust the sender and believe the content to be safe.

s22 (duplicate information)

From: Bond, Sally s47F(1) @servicesaustralia.gov.au>
Sent: Tuesday, December 23, 2025 9:39:15 AM
To: s47F(1) s47F(1) @kpmg.com.au>; Bond, Sally s47F(1) @servicesaustralia.gov.au>
Cc: s47F(1) @servicesaustralia.gov.au>; s47F(1) @servicesaustralia.gov.au>; Bond, Sally s47F(1) @servicesaustralia.gov.au>; s47E(d) @servicesaustralia.gov.au>; s47E(d) @servicesaustralia.gov.au>; s47E(d) @servicesaustralia.gov.au>

Subject: [EXTERNAL] FOR IMMEDIATE ACTION: KPMG information security incident [SEC=OFFICIAL]

s22 (duplicate information)

From: Bond, Sally
To: s47F(1)
Subject: RE: For Action: Request s47E(d) - Resolved [SEC=OFFICIAL]
Date: Wednesday, 7 January 2026 4:29:58 PM

Thanks s47F(1)

From: s47F(1)
Sent: Wednesday, 7 January 2026 3:57 PM
To: Bond, Sally
Cc: s47F(1) ; s47F(1)
Subject: FW: For Action: Request s47E(d) - Resolved [SEC=OFFICIAL]

Hi s47F(1)

FYI – Security team has also finalised the incident ticket today.

Kind regards

s47F(1)

From: s47E(d) @servicesaustralia.gov.au>
Sent: Wednesday, 7 January 2026 2:37 PM
To: s47F(1) @servicesaustralia.gov.au>
Subject: For Action: Request s47E(d) - Resolved [SEC=OFFICIAL]

Your incident has been resolved successfully.

Report a Security Incident

Request ID s47E(d)

Request title Cyber Security Incident- SA information sent outside of the agency's network/system.

Resolution - Resolved Successfully

The message from the resolving team is

*** *below is the update from record* s47E(d) ***

Thank you for reporting the security incident. We note Cyber Security have advised on this issue and classified accordingly. Please continue to report. Even if it seems small or harmless, reporting could help to prevent a major security incident from occurring.

You may accept or reject the resolution in mySupport, otherwise your request will be closed automatically after 7 days.

User ID	User Full Name

Requested for:	s47E(d)	s47F(1)
Requested by:	s47E(d)	s47F(1)

s47E(d)

From: Frewin, Alison
To: s47F(1) ;s47F(1) ;s47F(1) ;s47F(1) ;s47F(1)
Cc: Flinders, Chris; s47F(1) ;s47E(d) ; Bernroider, Adrian; Bond, Sally
Subject: Contract Manager: KPMG Notification of Significant Events [SEC=OFFICIAL]
Date: Friday, 29 May 2026 5:27:38 PM
Attachments: image001.png
AFR KPMG article 28-5-26.pdf
AFR KPMG article 26-5-26.pdf
guidance-regarding-management-of-notification-of-significant-events-and-breaches-of-the-supplier-coc.pdf
image003.png
image004.jpg

OFFICIAL

Good afternoon all,

I'm writing to provide advice from the Department of Finance (Finance) in relation to your contracts with KPMG. This afternoon, the agency received advice from Finance (included below) on a Notification of a Significant Event from KPMG. This notification relates to historical whistleblower allegations and subsequent actions taken by KPMG in investigating these allegations. For information, I have attached recent media reporting on this subject and included general advice from Finance on supplier requirements under Notification of Significant Event contract clauses (included in your contracts).

Importantly, you are **not required** to take any action at this point, as the agency will await further advice from Finance. Please feel free to reach out to my team s47E(d) @servicesaustralia.gov.au) if you require further information.

Kind regards,

Alison Frewin, National Manager, Procurement Branch
Phone s47F(1) Mobile s47F(1)
Procurement Branch
CHIEF FINANCIAL OFFICER DIVISION
s47F(1)

I acknowledge the Traditional Custodians of the lands we live on. I pay my respects to all Elders, past and present, of all Aboriginal and Torres Strait Islander nations.

Notification of Significant Event: KPMG

Dear entities,

The Department of Finance (Finance) advises that it has received a Notification of Significant Event (NoSE) under the Management Advisory Services (MAS) Panel Head Agreement from KPMG Australia (KPMG).

KPMG has advised that the notification relates to governance and conduct matters identified through ongoing investigations concerning historical whistleblower allegations. As outlined in the notification, KPMG has also advised of changes in senior leadership, including:

- the resignation of the Chief Executive Officer, s47F(1)
- the resignation of the National Managing Partner – Audit and Assurance, s47F(1)
- the appointment of an Interim Chief Executive Officer, s47F(1)

Finance is reviewing the notification in accordance with its responsibilities under the MAS Panel Head Agreement. At this stage, there is no action required by entities.

Finance will keep entities informed of any further developments.

Regards,

Strategic Contracting Branch | Procurement Division

Commercial Group | Department of Finance

E: s47F(1) @finance.gov.au | A: s47F(1)



OFFICIAL

OFFICIAL

Australian Government
Department of Finance

Guidance for the management of Notifications of Significant Events and breaches of the Commonwealth Supplier Code of Conduct

The purpose of this document is to provide guidance and encourage consistent assessment and action for any Notification of Significant Events (NoSE) and breaches of the Commonwealth Supplier Code of Conduct (the Code) in relation to Commonwealth procurement contracts. In this guidance, use of the word notification covers both notifications under the NoSE clauses and Code.

Under the Commonwealth procurement framework each entity is responsible for its own procurement and contract management processes and decisions to meet its business needs, in line with the Commonwealth Procurement Rules. This includes monitoring compliance, managing contract performance, identifying misconduct by suppliers (and undertaking necessary action) and managing any notifications.

This guidance provides high level advice on a process for responding to notifications. Depending on the nature of the goods or services being procured, whether a notification is classified as a significant event and/or breach of the Code will be at the discretion of the official/entity. Similarly, the severity of any significant event or breach will require the judgement of the official/entity and will be dependent upon a range of factors related to the specific contract.

Use of this guidance is optional, and the ultimate decision-making authority lies with each entity.

Introduction

The NoSE clause was introduced into the Commonwealth Contracting Suite and ClauseBank on 19 May 2023. The Code came into effect on 1 July 2024, mandated by the Commonwealth Procurement Rules for all Commonwealth forms of contract. Supporting clauses were published alongside the Code in the Commonwealth Contracting Suite and ClauseBank. For contracts that were entered into prior to the introduction of the NoSE clauses and Code, officials should strongly consider updating those contracts to include those clauses.

Receiving a notification

For those contracts that include the NoSE and/or Code clauses, officials may receive notifications from the supplier, another Commonwealth entity, or a third party. When handling a notification, it is important to consider the specific terms and conditions of the contract. Where the notification is not received from the supplier, the contract manager will need to approach the supplier to progress its consideration.

If multiple entities are notified by a supplier of the same significant event or breach, they may consider either coordinating a cooperative response, or an entity may

choose to respond on behalf of all notified entities, for example where a notification relates to a range of contracts entered into under a panel arrangement.

When receiving a notification, contract managers should engage with their legal and procurement teams for any additional processes and considerations that an entity has put in place.

Process for responding to a Notification of a Significant Event or a breach of the Commonwealth Supplier Code of Conduct

Phase 1 Identify and assess	• **Request** notification (if required) • **Receive** notification • **Assess** severity

Phase 2
Initial action
	• Undertake one, or a combination of the following actions:
	  ○ Request additional information
	  ○ **Watch and monitor**, reassess if necessary
	  ○ Issue a **warning**
	  ○ Request a **remediation** plan (proceed to phase 3) and consider **restricting** or **suspending** the supplier thoughout the remediation process
	  ○ If applicable, **contact** other entities that may have active contracts with the supplier
	  ○ Upfront **termination** for particularly severe incidents

Phase 3
Remediation
	• **Review** remediation plan
	• **Determine** next course of action:
	  ○ Accept remediation plan in its current state (proceed to phase 4)
	  ○ Request revised remediation plan
	  ○ Termination, if deemed necessary

Ongoing Communicate and monitor	• **Ongoing communication** with the supplier on the implementation of the agreed course of action • **Report** as required • **Ongoing monitoring** of the supplier's actions through regular communication and media monitoring • **Follow up** to ensure adherence and compliance to agreed remediation plan

Phase 1 – Identification and assessment

Step 0 – Request notification (if required)

- A potential significant event (event) under the NoSE clauses or a breach of the Code may be brought to the attention of a contract manager by a supplier, a third party such as the media, or may be noticed by the contracting Commonwealth entity itself. If a potential event/breach was identified without a *notice* by the supplier, contract managers may request the supplier provide a *notice* within 3 business days unless a different timeframe is agreed.
- Consider whether the potential event/breach should reasonably have been identified by the supplier and promptly communicated. If the supplier considers that an event/breach has not occurred, they may provide information to support that claim.

Step 1 – Receive notification

- A supplier must immediately notify contract managers on becoming aware of a potential event/breach. The *notice* should include a summary of the potential event/breach, the date it occurred, and details of the personnel involved.
- If the potential event/breach involves a contract under a panel arrangement, notify the manager of the panel. The panel manager may, at that time, seek to manage this process and provide guidance to the contracting entity on what further steps the entity should take.

Step 2 – Assess severity

- Gather all facts and evidence regarding the potential event/breach.
- Consider whether the notification consitutes a significant event under the NoSE clause and/or a breach of the Code. Consider escalating this determination to an appropriate delegate providing all relevent information for informed decision-making. If an event is not considered significant, you may notify the supplier that no further action is required.
- Media coverage can be useful in the initial identification of a potential event/breach but it may not be appropriate to solely rely on when determing whether it is an event/breach and assessing severity. Consider whether additional information is required.
- The supplier may provide information and context about the potential event/breach to assist in evaluating the severity. The entity may request this information from a supplier, and the response and transparency of the supplier can factor into the evaluation and remediation process.
- Consider contacting other stakeholders involved or affected by the event/breach, including other Australian Government entities who have active work orders with the supplier, to assess wider impact and gain perspective. Should you do so, be mindful of your privacy and confidentiality obligations and seek legal advice where necessary.

- Consider engaging other Australian Government entities who have active work orders with the supplier to discuss the severity.
- Evaluate the event/breach against each relevant criteria in the sliding scale of severity (refer Attachment A). Consider how the notification came to your attention; an event/breach proactively notified by a supplier may demonstrate capable monitoring and reporting procedures, while discovering an event/breach through the media may indicate a lack of transparency. Consider what existing controls are in place to manage the event/breach. Consider whether the event/breach was an isolated incident or if it may be part of a broader pattern or trend. Note that the circumstances of each event/breach is unique and should be assessed as such.

Phase 2 – Initial action

Step 3 – Determine initial course of action

Once the severity of the event/breach is determined, follow one, or a combination of the following actions and document the decision:

- **Note event/breach, watch and monitor for now, reassess if necessary**
  - If an event/breach was considered sufficiently minor that remediation was not considered necessary, the entity may choose to take no further action and monitor the situation to ensure that the event/breach does not increase in severity or frequency.
  - Alternatively, on receiving *notice* of an event/breach, there may be insufficient information to determine a course of action due to pending outcomes from examinations, inquiries, investigations or legal proceedings. If no initial action is considered appropriate, the entity may choose to monitor the situation and consider options until there is sufficient information to make an assessment.
  - Further information on monitoring is in Ongoing Phase, Step 7.
- **Issue a warning**
  - In minor instances, it may be considered appropriate to issue a warning to the supplier without taking further action. Ensure warnings outline potential consequences for any further similar events/breaches.
    - A warning will not always be a required action.
- **Request remediation plan**
  - In minor to moderate instances, a remediation plan may be requested by the contract manager. The remediation process should be proportional to the event/breach. It may be determined that delivery of goods and services can continue as usual throughout the remediation process.
  - A *notice* of an event/breach may be considered severe enough that it may be considered appropriate to restrict services or suspend business from occuring under the contract during the remediation process, in line with any

existing dispute resolution clauses. The impact to the Commonwealth should be considered when making this assessment, including potential effects on the delivery of policy objectives, service continuity, and whether alternative suppliers are available to mitigate disruption. Seek legal advice to ensure any restriction or suspension is managed appropriately. Consultation with key impacted entities may be considered appropriate prior to the suspension of a supplier.

- **Termination**
  - A breach of Code or NoSE clauses may be considered so severe that no amount of remediation will suffice and that termination is immediately warranted. If termination is to be considered, the contract manager must ensure this decision aligns with termination clauses of the relevent contract or arrangment, and all options to remediate have been considered. The decision to terminate is intended to be the final step, noting dispute resolution clauses may be available to the supplier with regards to this step.
  - When considering the option of termination, seek legal advice to ensure it is managed appropriately. Assess the impact to the Commonwealth. The contract deliverables may be something that can be picked up and resumed by another supplier, or all or a substantial proportion of the work done to date may be compromised which could impact key Commonwealth objectives, or the supplier may be the sole provider of the goods/services required.
  - Consultation with key impacted entities may be considered appropriate prior to any recommendation to terminate a supplier.
  - All decisions regarding termination should be made in accordance with the entity's Accountable Authority Instructions and any internal processes and policies.

Phase 3 - Remediation

Step 4 – Request remediation plan

- At the entity's discretion, the preferred format, content and complexity of the remediation plan can vary depending on the nature and severity of the event/breach. For minor incidents, concise email correspondence may be considered sufficient detail to constitute a remediation plan. More severe incidents may necessitate a thorough and comprehensive remediation plan that may seek changes to company policies or procedures. If requesting a remediation plan from a supplier, clearly communicate expectations of what success looks like while avoiding being unnecessarily prescriptive. The type of details requested in a remediation plan should be informed by the nature and circumstances of the incident, considering any information already provided or available.
- Consider which of the following factors are relevant when requesting a remediation plan in line with the relevant clause(s):

- how the event will be addressed in the context of the goods/services, including confirmation that the implementation of the remediation plan will not in any way impact on the delivery of the goods/services or compliance with other obligations under the contract
- how the supplier will ensure similar events do not reoccur
- any other matter reasonably requested.

- Additional information requested may include, but is not limited to:
  - the reasons the incident(s) occurred
  - the failings of current processes that led to the incident
  - disciplinary consequences of the incident
  - measures taken to minimise any further impact of the incident
  - monitoring and compliance mechanisms to identify and manage potential future events/breaches.

Step 5 – Review and assess remediation plan

- Assess the draft remediation plan. Consider whether the outlined remediation sufficiently addresses concerns regarding the severity of the incident. If the remediation plan is approved, determine whether the incident is entirely resolved or if further implementation actions are required by the supplier to embed business changes. The contract manager should ensure ongoing communication and monitoring activities support the supplier to implement changes (refer Ongoing Phase).
  - If the proposed draft remediation plan is considered insufficient in its current state, determine what adjustments would need to be made for the plan to be accepted.
  - If the proposed remediation plan can be approved incorporating some improvements then request a revised remediation plan and clearly outline what changes need to be made.
    - For the NoSE clause, suppliers must resubmit revised draft remediation plans for approval within 3 business days of the request unless a different timeframe is agreed.
- If a remediation plan fails to adequately account for the severity of an incident or if there are multiple failed attempts to agree on a sufficient remediation plan, suspension, restriction or termination may be considered appropriate actions for your entity to take.
  - When considering the option of termination, assess the impact to the Commonwealth. The contract deliverables may be something that can be resumed by another supplier, or a substantial proportion of the work done to date may be compromised which could impact key Commonwealth objectives, or the supplier may be the sole provider of the goods/services required.
- Consultation with key impact entities may be considered appropriate prior to any recommendation to terminate a supplier.

- Seek legal advice to ensure termination is appropriate and managed appropriately.
- Maintain appropriate documentation for all decisions, and the basis for those decisions.
- All decisions regarding suspension or termination should be made in accordance with the entity's Accountable Authority Instructions and any internal processes and policies.

Ongoing – Monitoring and follow-up

Step 6 – Communicate

- Communication between customers and suppliers is a key mechanism to ensure best practice is maintained and reduce the likelihood of events/breaches occurring in the first instance, or recurring following a notification.
- Communication with the supplier throughout remediation activities is critical to ensure the supplier understands the severity of the event, your entity's (and more broadly, the Commonwealth's) expectations of required actions, evidence of implementation, and future monitoring requirements.
- If the event/breach was in relation to a contract under a panel arrangement and the panel manager is not managing the process, keep the manager of the panel informed throughout the process.
- For panel managers, if a supplier was removed, restricted or suspended from a panel arrangement, communicate this update to users of the panel and provide guidance on engagements with the supplier. Consider any other stakeholders that may be worth informing, such as managers of other panel arrangements that the supplier contracts through.
- Consider your reporting obligations, including any internal protocols. For consultancy contracts above $2 million, notifications against the Code are required to be reported biannually for the Senate Order for Consulting Services.

Step 7 – Monitor

- There is an ongoing need throughout the term of any contract to monitor the ethical behaviour of suppliers, commensurate with the scale, scope and risk of the contract.
    - This requirement is especially pertinent in the aftermath of a notification of an event/breach.
- The contract manager should monitor the supplier's approach to the initial notification process, and initial actions required.
- Throughout remediation activities, the contract manager should monitor the reported outcomes of implemented actions, and ensure compliance with the agreed remediation plan. Depending on the nature and severity of the incident,

this may involve a simple acknowledgement of no further incidents to report, or it may require a more comprehensive monitoring and reporting arrangement.

- It may be appropriate to regularly check in with suppliers regarding resolved events/breaches to gain confidence in the supplier's ability to deliver contracted services, or to inform future procurement processes.
- The contract manager should consider establishing a system of continued monitoring.
    - Ensure situations being monitored are resolved or a final update is provided prior to concluding an arrangement with a supplier.
- Remain cognisant of the quantity and frequency of monitored situations and stay vigilant to identify any potential trends or patterns of concerning events or behaviour.

Step 8 – Post-remediation

- If a suspension or restrictions had been imposed under the contract as a result of an event/breach, consideration may be given to removing those limitations and returning to business as normal.
- Suspensions or restrictions may be accompanied by a timeframe or threshold to trigger evaluation to determine if it is still appropriate or necessary to continue restricting or suspending the business.
    - If a specific timeframe has been established, as the end date is approaching consider whether the supplier has demonstrated adequate remediation or evidence of compliance for the suspension or restriction to be lifted in full.
        - Should it be determined that the suspension or restriction should not be lifted in full, consider whether the suspension or restriction should be extended or removed in part.
- If a suspension or restriction is indefinite or determined by a key performance indicator or threshold, establish a schedule or reminder system to ensure reevaluation occurs.
- Following remediation, entities should consider whether ongoing engagement with the supplier is required to ensure sustained compliance. This may include updating contract key performance indicators to reflect remediation outcomes, adjusting the frequency of contract management meetings, or establishing periodic check-ins to monitor long-term behavioural change.

Attachment A – Sliding Scale of Severity

The following scale provides a high-level overview of factors that may influence the assessment of severity and potential options for remediation. It is intended as a guide only and should not be interpreted as prescriptive. Each event/breach must be evaluated in context, considering the nature of the incident, its impact, and the specific contractual arrangement.

	Minor	Moderate	Severe
Factors of severity	• Nil to minimal business impact	• Potential of substantial business impact	• Significant to severe business impact
	• Nil to minimal damage to reputation of business or Commonwealth	• Potential of some damage to reputation of business or Commonwealth	• Damage to the reputation of business or Commonwealth
	• No confidentiality concerns	• Some concerns around confidentiality practices	• Violation of confidentiality agreement
	• Any potential or actual conflicts of interest were declared and managed appropriately	• Potential or perceived conflicts of interest could have been more proactively declared but did not impact contract deliverables	• Conflict(s) of interest were mismanaged, not declared, or impacted the deliverables of the contract
	• Isolated or infrequent incidents	• Regularly occurring incidents	• Frequently or consistently occurring incidents
	• Anticipated or common occurrence in relevant industry	• Atypical in normal industry business practices	• Poor or prohibited practice in relevant industry
	• Incident identified and managed by existing processes	• Incident identified by existing processes	• Incident identified by the Commonwealth or a third party
	• Supplier was upfront, honest and prompt in notifying the contract manager	• Supplier was aware of the event/issue and failed to proactively notify the contract manager but was prompt to respond with comprehensive information when requested by the contract manager	• Supplier attempted to conceal the incident, failed to proactively notify the contract manager of the incident, and/or failed to provide information when requested.
Potential supplier remediation actions and/or consequences	Note and take no further action, or request formal correspondence from the supplier (e.g. email/letter) providing a brief description of: • how/why the incident occurred • how the incident was/will be managed by existing policies and procedures • additional information as requested, including proposed actions to avoid future recurrence, e.g. updates to internal processes / policies / procedures Communicate and monitor as required.	Request a remediation plan detailing: • the reasons the incident(s) occurred • the failings of the current processes that led to the incident • any disciplinary consequences of the incident • all measures taken to minimise the further impact of the incident • any planned changes to policies and procedures to prevent future re-occurrence The contract manager can deem the remediation plan insufficient and request further details. Communicate, monitor and follow up to ensure implementation of remediation.	Consider suspension or termination of contract. For arrangements not terminated, request a comprehensive remediation plan detailing: • the reasons the incident(s) occurred • the failing of the current processes that led to the incident • any disciplinary consequences of the incident • all measures taken to minimise the further impact of the incident • any planned changes to policies and procedures to prevent future re-occurrence • the establishment of a continued monitoring arrangement

From: s47F(1)
To: s47F(1)
Cc: s47F(1) s47F(1)
Subject: Notice of Significant Event
Attachments: image001.jpg
image002.jpg
image003.jpg
image004.jpg
image005.jpg

Hi s47F(1)

On Friday 29th May 2026, KPMG notified the Department of Finance formally of a notifiable significant event (under the Management Advisory Services (MAS) Panel) in relation to the inappropriate sharing of client documents on certain non-government engagements. We have taken this matter very seriously but I did want to confirm that the matters being reported do not involve any Commonwealth engagements.

Consistent with the requirements for Significant Event disclosure under the MAS Panel and our contract for the Reporting Model (clause C.C.22), I can confirm that:

- none of the matters subject to the Notice, and described further below, concern the performance of services (Reporting Models and Accounting Advice) to the Department.
- we have not identified any inappropriate access, usage, or disclosure of the Department's data or information in connection with the matters under investigation; and
- none of the Specified Personnel or other personnel engaged in connection with the Services to the Department were involved.

The matters raised relate to corporate audit engagements and proposals and do not relate to engagements for government clients. As this is still ongoing, KPMG continues to work with the Department of Finance to meet our obligations under the MAS panel and our contractual commitments to the Department.

I can assure you of the seriousness with which we take these matters and would appreciate the opportunity to explain how we maintain the confidentiality of the Department's information held or accessed by our team. If you would like more information, please let me know and if you have any other queries, I can be contacted at any time either via email or mobile

Kind regards

s47F(1)

s47F(1)

kpmg.com.au





From: s47F(1)
To: s47F(1)
Cc: s47F(1) ; s47F(1)
Subject: Notice of Significant Event
Attachments: image001.jpg
image002.jpg
image003.jpg
image004.jpg
image005.jpg

---

s22 (duplicate information)