The Institute of Internal Auditors Australia

Dear Q&A

Can a business unit impose conditions on internal audit when we request documents for an audit?

Our approved internal audit charter gives authority to internal audit staff to access any information, files and other documentation to enable internal audit to carry out its functions and activities. Despite this, for the first time ever, we have been requested by the area subject to audit to seek (a) approval from the privacy team and (b) confirm the information will be deleted on completion of the audit, otherwise the required data will not be provided.

Given the internal audit charter is inferior to the law in its authority (specifically the Privacy Act under which we are bound to follow the Australian Privacy Principles), should obtaining such approvals for internal audit data requests be a common practice or is the authority provided by the internal audit charter sufficient?

Answer

You rightly observe that legislative and regulatory requirements over-rule the internal audit standards and the situation you describe is quite common.

Some public sector internal audit charters include "subject to security requirements, the internal auditor has access to...". This is a reasonable provision in that it does not give the business the right to refuse access, but rather to ensure that the person gaining access has an appropriate level of security clearance.

Every organisation whether public sector or corporate has a duty to protect personally identifiable information from unauthorised use or disclosure. It seems reasonable that when you are requesting such information, you obtain the approval of the privacy team. In practice it is often possible to undertake the testing necessary without including fields that identify individuals – for example it might be possible to work with employee-IDs rather than with names or with postcodes rather than full addresses. Provided it is possible to trace back the de-identified record to its original, should an exception be noted, there is no harm done to the internal audit process.

You would ordinarily be aware if a data request involves extraction of personally identifiable information, so obtaining the approval of the privacy team need not become a normal part of the data request process. It should only be necessary to go there when the information might be sensitive.

It is more difficult to promise that the data will be deleted on 'completion of the audit' unless we are flexible about what this means. It is reasonable to promise to delete records when they are no longer needed for internal audit purposes, but some records may need to be kept as audit evidence. Once again, the records in their raw form are not necessarily useful – you are more likely to want to keep statistical analyses and similar processed results, and these are unlikely to hold anything of concern.

Need an answer? Send your questions through to IAassist@iia.org.au