Connect › Support › Advance

The Institute of Internal Auditors Australia

Whitepaper

Auditing Data Risk Management

January 2023

Level 5, 580 George Street, Sydney NSW 2000 | PO Box A2311, Sydney South NSW 1235
T +61 2 9267 9155 **F** +61 2 9264 9240 **E** enquiry@iia.org.au **www.iia.org.au**

Auditing Data Risk Management

Contents

Background

Purpose

Compared to other more established risk classes, data-related risk is a relatively new area of focus in which most organisations are still maturing their risk management approach. Due to increased digitisation of processes and reliance on data for decision-making and reporting, internal audit functions need to incorporate data risk management into their internal audit plans if they have not already done so. The challenge is to take a systematic and efficient approach to auditing management of data-related risk. This White Paper provides an overview of data-related risk management and discusses the key areas that should be covered when auditing it.

Background

Organisations are spending increasing amounts of time and effort unlocking powerful insights from their data. This is crucial for decision-making. In order to ensure data being analysed is accurate and fit-for-purpose across its end-to-end lifecycle, it is imperative to ensure data across the organisation is well-managed and well-governed.

There are two parallel aspects of data-related risk. We will use the term 'data risk' to cover both these aspects:

- Data must be fit-for-purpose and this implies the 'purpose' must be understood and 'fitness' defined. Some decisions require high accuracy, reliable data and others may accommodate some inherent uncertainty. This aspect may be regarded as 'data quality'. Data collected for one purpose will not necessarily be suitable for a different purpose.
- The processes by which information is collected and stored must be appropriate for the data quality being sought. Higher quality data is likely to have higher cost than lower quality data. It is counter-productive to spend more on the collection and storage of data than the end benefit to the organisation.

Having proper data risk management in place and sufficient staff with data risk management expertise has often been an after-thought for organisations, with many now playing catch-up. It is important for internal audit to ensure the business has effective data risk management processes and procedures in place. Poor management of data can lead to poor outcomes for the organisation.

Discussion

Issue

Data risk management is an emerging risk area requiring internal audit coverage to minimise the risk of unintended exposure of sensitive data, flawed decision-making, and inaccurate management and regulatory reporting. Regulators have increased their scrutiny of data risk management over past years and recent cyber-attacks where sensitive information for millions of customers were exposed have increased government sensitivity to these issues. This reinforces the need for organisations to have robust data management processes.

Auditing Data Risk Management

History

Good governance of data and the management of data risk are closely related.

For more established organisations, data has historically been managed in siloes partitioned by systems and business areas. Data was not consistently managed across these siloes and enterprise-wide data standards were not developed. The challenge for enterprise data teams has been to fix historical data management issues and to make sure data created going forward is properly governed.

The well-established international standard on information technology governance ISO/IEC 38500:2015 'Information technology – Governance of IT for the organisation' sets out a series of principles that have been adapted for data in ISO/IEC 38505-1:2017 'Information technology – Governance of IT – Governance of data – Part 1: Application Of ISO/IEC 38500 to the governance of data'.

Data Management Policy and Framework

The best starting point for the internal auditor is to review the data management policy and framework in place, if there is one. There is no 'one size fits all' approach for how an organisation approaches data management – in some organisations there may be an overarching framework supported by multiple policies or there may be a single comprehensive policy. The best approach is dictated by the size of the organisation, the volume, variety and complexity of data and regulation.

Data Governance

In a centralised model, a central data management office reporting to a chief data officer or an equivalent senior officer will own the policy and framework. As 'data' can mean different things to different people, the internal auditor should check whether there is a definition of what 'data' actually means for the organisation, including whether it covers both digital and non-digital records (such as hardcopy documents).

Roles and responsibilities for various teams should be defined including critical staff such as chief data officer, data risk management support staff. and 'data owners' or 'data stewards'[1]. Data steward will often be a part-time role incorporated into another job role – it may also be a full-time position, depending on the organisation.

Senior management may opt to oversee data governance through a dedicated committee in which members include senior data management staff across the organisation including the chief data officer and data stewards. If a dedicated committee does not exist, data governance can be included as a standing item in another relevant committee such as technology committee or risk committee.

Topics for discussion may include:

- Major data initiatives across the organisation.
- Metrics defining the current state of data risk management and future targets.
- Significant data-related issues.
- Major changes to the data management policy and framework.
- Major changes to senior data governance roles and responsibilities.

Data Partitioning and Stewardship

To facilitate enterprise-wide data risk management, data across the organisation may be divided in some manner. This process establishes a direct link between the business and the data. For example, in organisations providing products to customers with the aid of suppliers, data can be divided into the main business areas such as:

- Customers.
- Products.
- Transactions.
- Suppliers, business partners, etc.

Each data area will have a data steward accountable for it. If the data steward is a senior member of staff, they may be supported by delegates such as direct reports, risk professionals or specialist data governance staff who perform day-to-day management of data and periodically provide updates to the data steward.

Data stewards should receive sufficient training to ensure they understand their responsibilities and they should dedicate sufficient time and effort to execute their responsibilities. There should be a periodic assessment performed by data stewards that assesses the current state of data within their remit including data quality, known issues and progress of any data remediation projects.

In some organisations, a central team may have responsibility for data across the organisation. Irrespective of what data partitioning and stewardship structure is used, there should be clarity around the structure used and on roles and responsibilities.

1 As all data is actually owned by an organisation, we will refer to the individual with responsibility for making decisions about retention, access and use of data as a 'data steward'.

Auditing Data Risk Management

Data Quality

The definition of quality is driven by intended use of the data. Poor data quality is a common weakness across organisations, highlighting the need for a systematic approach to measuring data quality and providing visibility across the organisation. Data quality issues commonly arise when data collected for one purpose is adapted for a different business purpose.

For organisations regulated by the Australian Prudential Regulatory Authority (APRA), Prudential Practice Guide CPG-235 'Managing Data Risk' defines six main dimensions of data quality:

- Accuracy.
- Completeness.
- Consistency.
- Timeliness.
- Availability.
- Fitness for use.

For organisations not regulated by APRA, CPG-235 is still a useful reference for managing data quality. It is important to know the uncertainty in each of these dimensions. Data must be tolerably accurate for the purpose to which it is put, but it is possible to spend too much on data accuracy for the desired outcome. On the other hand, if the use of data is to be upscaled it will be important to know it is sufficiently accurate for the new purpose.

A robust data quality approach at a minimum involves periodic execution of data quality rules over an organisation's critical data. Data quality results should be communicated via reports or dashboards to relevant staff such as data stewards who can take action if data quality is not at an acceptable level.

In organisations where data quality is not consistently measured, management should be asked how they gain comfort over the organisation's data quality and what their approach is to identifying data quality issues, which can then be subject to remediation.

Data Criticality and Prioritisation

Due to the high volume, variety and complexity of data produced in today's business environment, it is important to identify data critical to the organisation and ensure the quality of this data is subject to strong controls and clear oversight. Criteria for determining what data is critical will vary from organisation to organisation, but includes factors such as:

- Data used in decision-making such as performance measures (KPIs), insights and reports presented to senior management and the board of directors.
- Data supporting financial statements.
- Data provided externally for example from customers, government and regulators.

Assuming the concept of critical data exists, there should be a catalogue capturing data element names and data element definitions. For example, customer critical data may be customer name, address and date of birth. Due to the dynamic nature of management reporting and regulatory obligations, it is important to check whether there is a periodic process (such as 6 months or 12 months) to reassess whether the current list of critical data is complete and accurate.

If critical data has not been defined, management should be questioned about this be asked whether there have been adverse outcomes identified due to a lack of critical data identification.

Data Classification and Security

Data should be classified according to how sensitive it is. At a minimum, data should be classified as being sensitive and non-sensitive. For example, personally identifiable information (PII) of individuals is very sensitive information and may be subject to legislated protection. In most organisations, additional classifications will be required.

Sensitivity criteria can be based on potential adverse outcomes associated with disclosure of data. For example, if customer PII data is unintentionally disclosed through a cyber-attack, adverse outcomes include:

- Privacy breach and associated penalties and fines.
- Increased likelihood of identity fraud for the compromised customers.
- Losing customers to competitors.
- Reputational damage if reported in the media.

Data classification determines the appropriate storage, access and transfer mechanisms for data. These processes are referred to as data security. Access to any data should be restricted to staff requiring access for legitimate reasons. however general access may be a cost-effective solution for non-sensitive data. The storage and transfer of some data may have special provisions driven by law or by sensitivity in which case strong encryption might be appropriate.

As data classification and data security requirements are a relatively new concept for most organisations, general awareness across the organisation outside data management and IT staff may be limited.

Auditing Data Risk Management

Data Privacy

PII is subject to provisions of the Australian Government 'Privacy Act'. Other jurisdictions have extra-territorial provisions in their privacy laws that might be applicable to Australian organisations. Data privacy breaches have increased in past years and have received widespread media attention through several high-profile incidents.

The Office of the Australian Information Commissioner (OAIC) is the national regulator for privacy. The OAIC regulates the 'Privacy Act' which covers how personal information is handled by organisations. If personal information is compromised through inappropriate access, insufficient data storage controls, or inadequate data transmission controls, a data breach may have occurred. The OAIC administers the Notifiable Data Breaches scheme which requires organisations to:

- Notify individuals if a data breach is likely to cause them serious harm.
- Report serious breaches to the OAIC.

Refer the OAIC website for more information on data privacy.

Data Issues

Most organisations have data-related issues, whether they relate to data completeness, accuracy, quality, security, privacy or some other data deficiency. What differs across organisations is how these data-related issues are identified, made visible to appropriate staff and remediated.

One approach is to use a risk management system to capture data-related issues and ensure there is an easy way to distinguish data-related issues from other issues. Sifting through free-text fields is not an ideal approach for identifying data-related issues due to the high potential for inconsistent descriptions of data-related issues. A more robust approach is the ability to tag data issues through a drop-down box or list.

If data issue tagging is available, it is possible to capture metrics on how well the organisation is tagging data issues, identifying trends over time, and whether particular business areas and systems have a higher proportion of data-related issues.

If a risk management system does not provide the ability to tag data issues, management should be questioned about how data-related issues are captured and actioned. Even if there is no robust approach, there may be widespread awareness of data-related issues, with staff having reduced ability to formally raise and therefore remediate such issues.

Conclusion

Summary

Organisations are starting to incorporate data risk management into their internal audit plans. This White Paper covers several areas that should be reviewed when auditing data risk management:

- Data management policy and framework.
- Data governance.
- Data partitioning and stewardship.
- Data quality.
- Data criticality and prioritisation.
- Data classification and security.
- Data privacy.
- Data issues.

Based on the size, complexity and nature of data management risks across an organisation, the areas discussed in this White Paper could be covered in multiple audits rather than a single enterprise-wide audit. Auditing data risk management could be a specific scope area in different audits.

Conclusion

Data risk is an emerging area for organisations. Having strong data risk management in place reduces the risk of flawed decision-making, adverse reputational impact from data-related issues, and regulatory scrutiny and fines. The areas covered in this White Paper should be used as a reference when auditing data risk management at your organisation.

Auditing Data Risk Management

Bibliography and References

Australian Prudential Regulation Authority, 2013. Prudential Practice Guide: CPG 235 – Managing Data Risk. [Online] Available at: https://www.apra.gov.au/sites/default/files/Prudential-Practice-Guide-CPG-235-Managing-Data-Risk_1.pdf

Institute of Internal Auditors, 2012. Practice Guide: Auditing Privacy Risks, 2nd Edition. [Online] Available at: https://global.theiia.org/standards-guidance/Member%20Documents/PG%20Auditing%20Privacy%20Risks.pdf

International Organization for Standardization & International Electrotechnical Commission, 2016. AS ISO/IEC 38500 Information technology - Governance of IT for the organization, Sydney: Standards Australia.

International Organization for Standardization & International Electrotechnical Commission, 2017. ISO/IEC 38505-1 Information technology — Governance of IT — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data., Geneva: ISO/IEC.

Office of the Australian Information Commissioner, 2014. Privacy fact sheet 17: Australian Privacy Principles. [Online] Available at: http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles [Accessed 20 Jul].

Office of the Australian Information Commissioner, n.d. Australian Privacy Principles. [Online] Available at: https://www.oaic.gov.au/privacy/australian-privacy-principles

Selmier, W. T. & Frasher, M., 2003. Differing views of privacy rights in the EU and U.S., and the resulting challenges to international banking: An interview with Joseph Cannataci. Business Horizons, Volume 56, pp. 779-786.

Purpose of White Papers

A White Paper is a report authored and peer reviewed by experienced practitioners to provide guidance on a particular subject related to governance, risk management or control. It seeks to inform readers about an issue and present ideas and options on how it might be managed. It does not necessarily represent the position or philosophy of the Institute of Internal Auditors-Global and the Institute of Internal Auditors–Australia.

Author's Biography

This White Paper written by:

Tariq Islam PMIIA, BEng(First Class Honours), BMaths&ComputerScience, DCAM

Tariq has 17 years of experience across financial services, professional services and defence, including 10 years of internal audit experience at CBA, Westpac and PwC. In 2023, Tariq founded RapidLynx Consulting to provide data analytics and data management consulting services to organizations in the Asia Pacific.

Prior to starting RapidLynx Consulting, Tariq held Executive Manager Analytics roles in internal audit at CBA and Westpac where he led teams delivering data analytics work across multiple audit teams. Across CBA and Westpac, Tariq led data analytics work on over 100 internal audits using traditional and emerging data analytics techniques to consistently identify material issues across all major business units and risk classes.

Before moving to banking, Tariq spent more than a decade working in risk and fraud analytics at PwC and defence engineering projects at BAE Systems.

This White Paper edited by:

Michael Parkinson BSc (Hons), Grad Dip Computing, PFIIA, CIA, CISA, CRMA, CRISC

About the Institute of Internal Auditors–Australia

The Institute of Internal Auditors (IIA) is the global professional association for Internal Auditors, with global headquarters in the USA and affiliated Institutes and Chapters throughout the world including Australia.

As the chief advocate of the Internal Audit profession, the IIA serves as the profession's international standard-setter, sole provider of globally accepted internal auditing certifications, and principal researcher and educator.

The IIA sets the bar for Internal Audit integrity and professionalism around the world with its 'International Professional Practices Framework' (IPPF), a collection of guidance that includes the 'International Standards for the Professional Practice of Internal Auditing' and the 'Code of Ethics'.

The IIA-Australia ensures its members and the profession are well-represented with decision-makers and influencers, and is extensively represented on a number of global committees and prominent working groups in Australia and internationally.

Auditing Data Risk Management

The IIA was established in 1941 and now has more than 200,000 members from 190 countries with hundreds of local area Chapters. Generally, members work in internal auditing, risk management, governance, internal control, information technology audit, education, and security.

Copyright

Disclaimer