REPORT 592

# Review of ASX Group’s technology governance and operational risk management standards

September 2018

## About this report

This report outlines the findings of a review of ASX Group’s technology governance and operational risk management standards. We foreshadowed our intention to undertake this wider (non-incident driven) review following our review of the ASX equity market outage in September 2016.

This report makes a number of recommendations. These are designed to improve ASX Group’s technological and operational risk management arrangements so that it is better able to meet the expectations of its customers, its regulators and the wider users of the Australian financial market. Many of the findings and recommendations from the review will be relevant to other important financial sector organisations regulated by ASIC.

### About ASIC regulatory documents

In administering legislation ASIC issues the following types of regulatory documents.

**Consultation papers**: seek feedback from stakeholders on matters ASIC is considering, such as proposed relief or proposed regulatory guidance.

**Regulatory guides**: give guidance to regulated entities by:

- explaining when and how ASIC will exercise specific powers under legislation (primarily the Corporations Act)
- explaining how ASIC interprets the law
- describing the principles underlying ASIC's approach
- giving practical guidance (e.g. describing the steps of a process such as applying for a licence or giving practical examples of how regulated entities may decide to meet their obligations).

**Information sheets**: provide concise guidance on a specific process or compliance issue or an overview of detailed guidance.

**Reports**: describe ASIC compliance or relief activity or the results of a research project.

## Disclaimer

This report does not constitute legal advice. We encourage you to seek your own professional advice to find out how the Corporations Act and other applicable laws apply to you, as it is your responsibility to determine your obligations.

Examples in this report are purely for illustration; they are not exhaustive and are not intended to impose or imply particular rules or requirements.

# Contents

# A Executive summary

**Key points**

Following our incident-specific review of the ASX equity market outage in September 2016, we foreshadowed our intention to undertake a more extensive review of ASX Group's technology governance and operational risk management arrangements. This review was conducted with the help of KPMG, a third party which ASX Group appointed and which also reported to both ASIC and the RBA.

Based on the findings from the review, we concluded that improvements in ASX Group's technology governance and operational risk management capabilities are required for it to fully meet regulatory expectations.

## Background

1 Well-functioning financial market infrastructure is critical to the integrity and reputation of the Australian financial market and the trust and confidence investors have in it. As the primary—and in some parts of the market, the only—market infrastructure provider in Australia, ASX Group has a critical role to play.

2 Given the overwhelming extent to which it relies on technology to deliver its services, robust technology governance and operational risk management is central to ASX Group's effectiveness as a market infrastructure provider. This is also one of ASX Group's key obligations as the holder of two market and four clearing and settlement (CS) facility licences.

Note: ASX Group is required to ensure its securities and futures markets operate in a fair, orderly and transparent way (s792A(a) of the *Corporations Act 2001* (the Corporations Act)) and that its four licensed CS facilities are fair and effective (s821A(a) of the Corporations Act). All of its licensed businesses are required to have sufficient resources (including financial, technological and human resources) to operate the market or CS facility properly (s792A(d) and s821A(d) of the Corporations Act).

3 Following the ASX equity market outage in September 2016, we undertook an extensive review of ASX Group's operational and technological management of that incident. In Report 509 *Review of the ASX equity market outage on 19 September 2016* (REP 509) we made a number of important recommendations for both ASX Group and ASX market participants. We also foreshadowed our intention to undertake a wider (non-incident driven) review of ASX Group's management of technology governance and operational risk.

4 We indicated that we might draw on the expertise of a third party to help with that review. At ASIC's and the RBA's request, ASX Group tendered for the appointment and selected KPMG for this purpose. As the RBA

oversees the stability of CS facilities operating in Australia, with a view to managing systemic risk, the RBA worked closely with ASIC during this review. Both ASIC and the RBA acknowledge the cooperation of ASX Group during the review and since its completion.

5 This report contains the observations, findings and recommendations of the review, as well as a number of associated observations from our ongoing oversight of ASX Group's market and CS facility licensees.

## Observations and findings

6 Historically, ASX Group's arrangements for managing operational and technological risk have served the Australian market well. The uptimes for ASX systems have, for example, consistently been in line with global best standards.

7 However, technology and operational systems across financial market infrastructure providers and the broader financial services sector are becoming increasingly complex and interconnected. It is critical that ASX Group can continue to meet the technology governance and operational risk management expectations of its customers and regulators in this dynamic environment.

8 The review benchmarked ASX Group's technology governance and operational risk management arrangements against internationally recognised technology governance and risk management standards.

9 The review identified areas for improvement. It found ASX Group's practices were more comparable to those of other exchanges in the global financial market infrastructure industry but lagged behind better practices in the broader financial services sector.

10 Given the critical role that ASX Group plays in maintaining the trust and reputation of the Australian financial market, it is important that it targets the better practices applied in the broader financial services sector.

11 ASX Group recognises the areas for improvement identified in the review. It is undertaking an extensive work program to implement all of the recommendations and had commenced work on almost half of them either before the review started or before the recommendations were finalised.

12 More broadly, the ASX board has placed additional focus on risk over the last year and, independently of this review, ASX Group has also taken steps to improve its technology governance and operational risk management. This included the appointment of several key senior executives across enterprise risk and technology, as well as making changes to internal governance arrangements.

13 These internal changes included bringing ASX Group's operations and technology teams together under the newly created Chief Operating Officer role and reshaping its committee structure to support improved senior executive and board decision-making, as well as accountability for operational and technology incidents. ASX Group has also adopted new technology and enterprise risk management plans, which were initiated prior to the review, has commenced staff recruitment and risk management awareness training and is in the process of identifying fit-for-purpose software tools to support these processes.

## Conclusion

14 ASX Group expects it will take up to three years to fully implement and embed all the recommendations from the review. It anticipates a significant component of the action items in this work program will be completed by the end of 2018.

15 The work program arose from the recommendations of the review as well as from other actions separately identified by ASX Group. It is designed to ensure ASX Group's technology governance and operational risk management standards are at the level necessary to fully meet the challenges and expectations of regulators and customers.

16 The work program is also designed to ensure commitment and accountability across a wide range of key performance areas that are also relevant to other financial institutions ASIC regulates. These include:

(a) a robust and effective 'tone from the top' on operational and technological risk management activities that reflects strategic sharpness and a clear, enterprise-wide perspective—and has the associated resourcing and accountabilities to make it meaningful;

(b) strategic investment in foundational, enterprise-wide capabilities to ensure that staff, internal systems and data support the board and senior management to readily identify risks, draw connections between business areas and make informed strategic decisions;

(c) an enterprise-wide technology strategy and associated enterprise architecture to support the delivery of new robust technology solutions—including a robust program to routinely monitor and evaluate existing core technology systems and assets; and

(d) a mature defence against risk management failure where accountabilities and responsibilities are clear and effectively understood—with a focus on ensuring appropriate resourcing is in place, particularly in the enterprise risk management function.

## Next steps

17 The program of work that ASX Group is undertaking is being closely supervised by ASIC and the RBA.

18 Many of the findings and recommendations from this review will be relevant to other financial services sector organisations regulated by ASIC. We encourage the boards and senior management of these other organisations to critically review their own technology governance and operational risk controls and to evaluate this report's findings and recommendations in the context of their own business.

# B Background to our review

**Key points**

We foreshadowed this review in our public report on the ASX equity market outage in late 2016. During that outage and since, other technology and operational incidents have also highlighted the need for improvements to the organisation's technology governance and operational risk management framework.

The review paid particular attention to ASX Group's operational risk management, technology governance, enterprise architecture and incident management.

## Background

19 In September 2016, ASX Group experienced a major trading system outage that impacted the entire Australian equities market. Our review of that outage identified a number of failings on the part of ASX Group. These included technological and operational issues which were compounded by instances of human error. Our assessment of that incident was outlined in REP 509 and included several recommendations for ASX Group and ASX market participants.

20 Since that incident, we have continued to work closely with ASX Group, market participants, industry associations and other market operators on a range of remedial steps designed to address important issues exposed by the circumstances on that day. In parallel, and as part of our ongoing oversight of ASX Group, we have also observed further operational and technological risk-related incidents.

21 While no one incident has been as structurally severe as the equity market outage of September 2016, the frequency and breadth of the incidents—across the Australian listing, trading and post-trade environments—gave ASIC cause for concern. The way in which ASX Group had characterised, evaluated and responded to certain incidents also concerned us.

## Context

22 It was in this context that ASIC and the RBA requested ASX Group to tender for the appointment of a third party to help with this review—and

KPMG was selected. The review paid particular attention to ASX Group’s practices and arrangements for:

(a) operational risk management;

(b) technology governance;

(c) enterprise architecture; and

(d) incident management.

# C Risk management

**Key points**

Effective enterprise risk management is increasingly accepted as a crucial component for the delivery of strategic value within an organisation. A robust and embedded enterprise risk management framework demands a strong ‘tone from the top’, to which the ASX board has re-affirmed its commitment.

This review has identified important opportunities for ASX Group to strengthen the operational risk management component of its enterprise risk management framework. Additional risk resources, such as specialist staff and risk analysis tools, along with a strong risk culture, are also central for further improvement in ASX Group’s operational risk management capabilities.

## Overview

23 Over the past few years, there has been a marked ‘step change’ in the recognition given to the important role of enterprise risk management in the financial services sector.

24 Those organisations at the forefront of this positive change have been characterised by boards and senior management that recognise the strategic value that can be delivered by an embedded, high-quality enterprise approach to operational risk management. Doing so aligns with better practice, as articulated in the recent update to the Committee of Sponsoring Organizations of the Treadway Commission’s enterprise risk management framework (COSO ERM).

25 For market infrastructure providers that are meeting good practice standards, this shift to maturing risk management practices complements the traditional attention given to managing the potential risk of counterparty default or settlement failure (otherwise known as clearing or settlement risk).

## Observations and findings

26 During this period of exponential improvement across parts of the financial services sector, ASX Group has taken steps to improve aspects of its broader enterprise-wide risk management framework. This has included the important appointment of a new Chief Risk Officer with an enhanced enterprise-wide risk management mandate and responsibility.

27 A robust and embedded enterprise risk management framework demands a strong ‘tone from the top’, to which the ASX board has re-affirmed its commitment. Organisations that have a strong ‘tone from the top’ can point to:

(a) a clear and effective articulation by the board and senior management of the organisation’s strategic risk appetite;

(b) a ready demonstration by the board and senior management of performance against that framework;

(c) strategic, committed and meaningful resource allocation to enable the effective delivery of that framework; and

(d) supporting processes such as business planning and performance agreements throughout the organisation which ensure measurability and accountability against that framework.

28 ASX Group recognises the need for improved articulation of its strategic risk appetite and the refinement of its key risk indicators (KRIs) to help the organisation monitor and manage enterprise risk. The board and senior management have recently been involved in work to develop a revised risk appetite statement and a clear strategy and roadmap for maturing ASX Group’s risk management approach.

29 In addition, ASX Group’s leadership team has been providing further and more regular communications to staff on the importance of robust operational and technology risk management. This reflects the renewed strategy and commitment being driven by a three-year enterprise risk management plan.

30 As part of its focus on improved enterprise risk management (and before the review commenced), ASX Group simplified various elements of its governance and management committee structure. This simplification was designed to clarify roles and enhance accountability on issues relating to enterprise risk and project management and was welcomed by ASIC.

31 ASX Group is also committed to the strategic allocation of resourcing to support the delivery of this focus on risk management, including strengthening its ‘three lines of defence’ model.

Note: ASX Group follows the ‘three lines of defence’ model for risk management:

- first line of defence—the specific risk functions performed by operational management and staff;
- second line of defence—a dedicated risk management and compliance function; and
- third line of defence—internal and external audit.

32 Steps are currently underway to increase the clarity of responsibilities and accountabilities within the three lines of defence. This is coupled with an increase in resourcing across the first and second lines, particularly within ASX Group’s second line function.

33 An associated focus area for delivery of an effective enterprise risk management framework is to identify and break down any internal silos that have the potential to impede enterprise-wide risk identification and result in fragmented solutions. To help with this, it is important to:

(a) have an effective central risk register that can capture enterprise-wide risks for further analysis; and

(b) ensure that forensic root cause analysis of the risks on the register is embedded within the organisation as standard practice.

34 The use of data and effective software tools to support risk management activities and provide insight for internal risk reporting purposes is also critical. As part of this, it is important that, where appropriate, analysis can attribute multiple causes to an incident and that issues are allocated to well-considered headings and categories.

35 Although industry-wide developments in the measurement of risk culture are at an early stage, this is also an important space for firms to monitor and one that has the potential to offer increased risk management capability as it matures.

## Recommendations

36 Table 1 sets out a summary of the steps ASX Group is focusing on to further improve its enterprise-wide risk management practices. This also forms part of the current ASX Group work plan that ASIC and the RBA are closely monitoring. ASX Group had already commenced some elements of this work prior to the review or had identified plans to do so.

37 We encourage all other important financial institutions we regulate to evaluate the maturity and effectiveness of their own enterprise risk management practices against the set of initiatives in Table 1—and to consider the application of this report's findings and recommendations in the context of their own business.

38 Those other financial institutions should, for example, consider the utility of applying recognised risk management frameworks (such as COSO ERM or the International Organization for Standardization's ISO 31000:2018 *Risk management—Guidelines* (ISO 31000:2018)) to their operations.

Note: The ASX corporate governance principles and recommendations (PDF 1.41 MB) also sets out recommended corporate governance standards for ASX-listed entities with an important emphasis on risk management governance and practices. See, for example, *ASX corporate governance principles and recommendations*, 3rd ed., Principle 7: Recognise and manage risk, which states that ultimate responsibility for a listed entity's risk management framework rests with the full board (p. 28).

Table 1: Steps to further improve ASX Group's operational and technology risk management

| | |
|---|---|
| **Risk appetite statement** | Refresh the risk appetite statement and execute a plan to further operationalise it throughout the organisation, including documenting the formal consideration of risk appetite in strategy and key business decisions |
| **Enterprise risk management plan** | Continue to roll out the new three-year enterprise risk management plan as developed by the risk management function |
| **Strategic risk communication** | Continue to roll out the risk communication plan to support the delivery of the three-year enterprise risk management plan, and support the embedding of a risk management culture within the organisation |
| **Holistic approach to risk management** | Develop a holistic view of all policies, processes, procedures and controls to enable more effective assessment and management of risk |
| **Risk resourcing** | Continue to increase risk management resourcing for first and second lines of defence, in accordance with the three-year enterprise risk management plan, to ensure adequate risk resourcing is in place |
| **Technology risk function** | Continue to develop and mature the first line risk function in technology to ensure technology (and operations) are aligned with the second line risk function |
| **Performance accountability** | Include more detailed risk management performance goals in management and staff performance plans |
| **Risk culture measurement** | Develop measures to track, monitor and assess the impact of risk initiatives on culture. Once embedded, this should support enhanced internal reporting to executive management and the board |
| **Risk management in key business processes** | Continue to embed risk management into key business processes such as strategic planning, project management and performance management activities. Consider the appropriateness of advanced risk assessment tools |
| **Approach to project management** | Continue to enhance the consideration of risk in project management |
| **Enhanced risk reporting** | Enhance risk reporting to include additional analysis of risk information, for example the development of a revised risk reporting format and deeper risk analysis insights. This could include taking account of:<br>• internal feedback from areas such as general management and the audit and risk committee; and<br>• analysis of common cross-functional and cross-divisional risk causes, controls and actions |
| **Enhanced key risk indicators and reporting dashboard** | Finalise the development of a simple and informative KRI dashboard. Continue the development of risk monitoring tools and KRIs to more effectively monitor key risks |
| **Governance, risk and compliance (GRC) system** | Progress current and future business requirements for a GRC system that will support the organisation's risk framework. Embed the GRC system into the organisation's reporting functions |

# D Technology governance

**Key points**

An organisation that is heavily dependent on technology to maintain its sustained success, such as ASX Group, must have effective technology governance practices in place. The review identified areas for improvement in ASX Group technology governance processes, including technology strategy, program management, resource management, IT risk management capability and supplier governance frameworks.

ASX Group commenced work on some of these issues prior to the review and will continue to progress those and others as part of the work program arising from the review's recommendations.

## Overview

39 The embedded nature of technology in almost every aspect of global financial services today makes effective technology governance a critical feature of the sustained success of any organisation.

40 A number of internationally recognised frameworks are available to evaluate the effectiveness of an organisation's technology governance. Examples of widely used frameworks include ISO/IEC 38500:2015 *Information technology: Governance of IT for the organisation* and ISACA's COBIT 5 (Control Objectives for Information and Related Technologies). As a general observation, we expect boards and senior management of all important financial institutions we regulate to be familiar with the framework(s) adopted by their organisation and the relative effectiveness of those framework(s) for their business.

41 For this assessment, selected components of COBIT 5 were used as a reference framework. That framework provides a number of valuable measures for assessing the effectiveness of an organisation's technology governance and describes an effective technology governance framework as:

(a) providing clear direction to ensure that technology investments support the business;

(b) an effective way to manage associated change;

(c) creating value for the business in alignment with enterprise objectives; and

(d) addressing the complete life cycle of IT investment.

## Observations and findings

42 ASX Group is continuing to make improvements across key technology governance processes. It had previously recognised the need to make these improvements and is continuing its work to address these areas.

43 An important area for strategic attention from the board and senior management of any financial institution is the organisation's technology strategy. At a minimum, a robust technology strategy should be aligned to the organisation's business strategy and clearly set out an overarching vision for the technology function, as well as meaningfully articulate the uplift in capability needed to deliver the vision across the business.

44 Another important area for board and senior management attention is the effectiveness of the formal enterprise architecture (EA) function and enhanced governance functions to support decision-making processes. This is discussed in more detail at paragraphs 53–59. A comprehensive EA can deliver the blueprints and roadmaps that underpin business and technology strategy.

45 An immature EA function can undermine an organisation's ability to effectively plan and execute new or enhanced business and technology strategies over the medium to longer term. The maturing and increased effectiveness of this function is also advanced by ensuring there is clarity about the role of EA in the strategic planning processes.

46 With the September 2017 recruitment of a Chief Information Officer to fill this vacant position, the ASX Group five-year technology strategy has now been revised. ASX Group has confirmed this strategy will be supported by a formal capability gap analysis (covering both resourcing and group skill set) across all technology functions.

47 It is also essential that boards in the financial services sector have a strategic understanding of their businesses' technology performance. There has been an observed increase in the coverage and detail of information provided to the ASX board on technology performance and related matters. Recent reporting to the ASX board has, for example, emphasised an important risk assessment of the current state of key system assets. This type of reporting underpins the critical information flows needed to support appropriate technology governance and accountability.

48 Reporting at a more summarised level to any board is to some extent necessary, but detail about considered options, strategic analysis and justification for the recommended decisions should also be included to assist boards in their active, critical and strategic understanding of this key performance measure.

49 Our experience is that effective board reporting is generated, at least in part, by:

(a) a strong 'tone from the top' which emphasises a demand for clearer information to support strategic board decision-making; and

(b) the skills and capability at the board level to meaningfully interrogate and evaluate the information being reported.

50 Below the board level in any financial institution there is also a need to align team structures and roles to better support team accountabilities and integration. As part of this exercise it is important that roles and associated responsibilities are documented and widely communicated. Improved supplier governance and contract management is also a critical area for ongoing attention and accountability.

## Recommendations

51 Table 2 sets out a summary of the steps ASX Group is focusing on to further improve its approach to technology governance. This also forms part of the current ASX Group work plan that ASIC and the RBA are closely monitoring. ASX Group had already commenced some elements of this work prior to the review or had identified plans to do so.

52 We encourage all other important financial institutions we regulate to evaluate the maturity and effectiveness of their own technology governance arrangements against the set of initiatives in Table 2—and to consider the application of this report's findings and recommendations in the context of their own business.

**Table 2: Steps to further improve ASX Group's technology governance**

| | |
|---|---|
| **Governance forums and practices** | Continue to uplift and expand the governance structure to incorporate:<br>• technical design and compliance, EA, a design authority and technical working groups (including cross-functional teams);<br>• clarification of roles and the processes and tools necessary to support efficient and sustainable governance reporting; and<br>• detailed documented analysis contained in key governance reports, including evidence of risk outcome assessment for recommended options/decisions taken |
| **Review of technology target operating model (TOM)** | Complete development of TOM to ensure team structures and roles are aligned and stable across key operational domains, in order to clarify and support team accountabilities and integration points in the design, build and run (operate) functions<br>Document and communicate all key roles throughout the organisation |

| | |
|---|---|
| **Technology strategy and capability roadmap** | Continue development of a current/future state technology capability model that aligns to business domains. Continue to ensure that technology strategy aligns to the organisation’s strategic plan and develop additional enterprise capacities as required. Develop success criteria and measures for regular reporting to executive management and the board on progress and directional changes of the technology strategy. Communicate changes to the technology strategy across all technology and business unit teams |
| **Enhance program management frameworks and compliance** | Ensure the program management framework addresses the organisation’s expectations regarding risk assessment and organisational risk outcomes (beyond risks to project delivery) as part of project planning, reporting and root cause analysis for change requests<br>Continue to ensure execution frameworks for low risk/low impact business and technology enhancements are appropriate and deliver consistent quality and design standards across all system changes |
| **Staff resource management** | Monitor that IT TOM delivers a single, integrated channel for planning resource demands across change activities, including projects, business and technology enhancements, systems fixes and business-as-usual initiatives<br>Establish processes for the periodic revalidation of the technology resource plan as part of ongoing technology strategic planning. Assess the impact of implementing project/change initiatives on staff resources |
| **Enhanced IT service management software tools and practices** | Continue initiatives to ensure change management and knowledge management functions are supported by appropriate software and repository tools, including a configuration management database with associated automated monitoring/compliance tools, a specialised change management solution and automated incident management capability<br>Align and update knowledge repositories to enable an end-to-end view of asset management, software licensing, system operations and integration and data flows for each service area/domain |
| **Enhance the supplier governance framework** | Define and document an end-to-end supplier governance framework to reflect all aspects of the supplier engagement life cycle. Ensure the supplier governance framework is integrated with existing frameworks (e.g. procurement framework) |
| **Mature key risk indicators for technology reporting** | Continue to ensure the KRIs used for monitoring and reporting technology risk reflect changes to the risk management approach of the organisation. Ensure the breadth of KRIs, including use of leading indicators, is sufficient and they contain defined targets and thresholds, which are benchmarked against current performance levels |
| **Formal technology controls register** | Continue to consolidate all technology controls into a single register aligned with industry standards (e.g. COBIT 5) and agree ownership of controls. Establish a formal review cycle as well as self-assessment of control appropriateness and effectiveness |

# E Enterprise architecture

**Key points**

An effective EA function provides a conceptual blueprint that captures the structure and operation of an organisation and is an essential component of an integrated, technology-driven business. EA aids in determining how best to achieve current and future capabilities while managing risks and interdependencies.

ASX Group recognises the importance of a robust EA and that structural and cultural change is required to further mature this function to support the effective delivery of its technology roadmap.

## Overview

53 An effective and robust EA function is essential in any integrated and technology-driven organisation, especially one that is delivering technological change. It provides a conceptual blueprint that captures the structure and operation of an organisation and aids in determining how best to achieve current and future capabilities while managing risks and interdependencies.

54 A good EA should be cohesive and clearly map the business and technology capabilities of an organisation, as well as articulate the organisation’s governance principles. It should also promote organisational alignment. Delivered effectively, it is instrumental in supporting an organisation’s strategic planning by driving long-term decision-making and steering a course towards its target state objectives. It also:

(a) allows for an enterprise-wide understanding of business process changes and their impact on technology; and

(b) helps with streamlining systems and processes and facilitates interoperability across an organisation.

55 Over time, effective EA will improve operational efficiency, lower costs and help minimise errors.

## Observations and findings

56 Given ASX Group’s central role in the Australian financial ecosystem, an effective EA function is critical in supporting its ability to make robust assessments of the extent to which strategic technology decisions will impact investors in, and users of, that system.

57 ASX Group has recognised that its technology planning had been influenced more by specific projects and business initiatives than true end-to-end enterprise considerations. This has resulted in the identified need for a more mature EA function to support the enterprise-wide planning process, with a more cohesive strategic lens and solution.

58 While key staff demonstrate strong domain-specific knowledge and the ability to consider application and physical architecture areas, major technology dependencies and sequential considerations have not always been effectively identified or managed across the broad ASX Group.

59 ASX Group recognises the importance of a robust EA and that it needs to operate a unified enterprise-wide architecture to most effectively deliver on its technology roadmap. ASX Group has developed a cohesive vision statement which will help to set the mandate and role of its EA in future strategic planning.

## Recommendations

60 Table 3 sets out a summary of the steps ASX Group is focusing on to further improve its approach to EA across the organisation. ASX Group had already commenced some elements of this work prior to the review or had identified plans to do so. The work in Table 3 also forms part of the current ASX Group work plan that ASIC and the RBA are closely monitoring.

61 We encourage all other important financial institutions we regulate to evaluate the maturity and effectiveness of their own EA (or equivalent) arrangements against the set of initiatives in Table 3, and to consider the use of suitable EA frameworks (where appropriate) such as the Open Group Architecture Framework or the Zachman Framework for Enterprise Architecture—and to consider the application of this report’s findings and recommendations in the context of their own business.

**Table 3: Steps to further improve ASX Group’s enterprise architecture**

| | |
|---|---|
| **Application of enterprise architecture in business planning** | Mature and ingrain the dedicated vision/mission statement and related principles that frame the mandate of EA within the day-to-day operations of the organisation, and particularly in strategic planning. Ensure EA plays a primary role in:<br>• planning the ongoing management of existing technology;<br>• selecting and deploying new technology and enhancing operational capabilities; and<br>• coordinating enterprise-wide innovation |

| | |
|---|---|
| **Target state architecture blueprints** | Develop enterprise level architecture blueprints defining the current state and future state planning for the organisation's conceptual/contextual models. Ensure blueprints cover each of the respective domains, including business, information, application and technology architecture<br>Define a suitable inventory of technology model definitions (e.g. logical and physical architecture), as required by each domain, to articulate an overall three- to five-year plan |
| **Roadmap of IT innovation initiatives** | Continue to develop EA capabilities and capacity, independent of business/system projects, to allow for an independent development pathway for IT innovation. Document a roadmap for the development of IT capabilities across each EA domain |
| **Dedicated enterprise architecture capability** | Continue to enhance the skills and capability of the EA function to supplement current solution architecture practices, supported by dedicated EA resources, independent of solution architecture roles |
| **Governance authority for enterprise architecture** | Embed the design authority function to provide decision-making governance over technology projects and domain-based designs. Establish architecture working groups across relevant EA domains (e.g. business architecture, application architecture, data architecture and technical architecture). Ensure timely and effective engagement with the architecture governance authority for project management and system enhancement design decisions |
| **Enhance the capture of architecture knowledge** | Effectively capture architecture design decisions in EA templates by including decision rationale, alternative options, impact and technology target state blueprint links. Decisions able to be readily referenced for future planning purposes and processes defined for the ongoing maintenance of architecture blueprints in the event of future changes<br>Develop an integrated, end-to-end view of the IT environment (e.g. data flows, systems, interfaces and infrastructure) across domain/process flows by integrating existing sources of architecture knowledge and supplementing these with additional overview documents (including templates) where required |

# F Incident management

**Key points**

ASX Group has historically demonstrated a strong record of platform reliability by global standards. It also has a strong track record of responding to, and addressing, specific incidents that arise from discrete operational and technological failures.

However, the review identified an over-reliance on subject matter experts, as opposed to well-established processes and procedures.

While ASX Group can point to enhancements over recent times, the review identified the need to improve its incident record keeping and the quality and accuracy of data creation, data retention and presentation.

## Overview

62 Strong and robust incident management practices are a core foundational element of any effective operational risk management framework. They position an organisation to respond effectively to issues as they occur. They also enable an organisation to pre-empt issues and reduce their number and impact over time by delivering key insights through strategic analysis and 'lessons learned'.

## Observations and findings

63 ASX Group has historically demonstrated a strong track record of reliability across its platforms, with an average system uptime of 99.9% for its top 23 critical systems over the past 12 months. These kinds of headline performance levels have served the Australian market well over an extended period.

64 ASX Group also has a strong track record of responding to, and addressing, specific incidents that arise from discrete operational and technological incidents. The review identified one reason for this as the strong domain corporate knowledge retained by specific staff and a cultural commitment to resolving operational incidents as they occur. Similarly, some incident management practices in parts of ASX Group were identified as exceeding industry norms.

65 For some time ASX Group has recognised the need to enhance its policies, procedures and software tools in order to deliver a more holistic and integrated understanding of incidents and systems availability and to support informed discussion about root causes and 'lessons learned'. In the period before the equity market outage in September 2016, for example, it

undertook an internal review of its incident management reporting arrangements.

66 Nevertheless, as highlighted in REP 509, we were concerned that ASX Group remained behind industry better practice in its broader approach to incident management. Even though ASX Group has taken steps to improve its approach, such as the merging and alignment of certain internal incident management processes across business lines, it still needs to make important improvements in this core area of operational risk management.

67 It is important that ASX Group's incident management arrangements are not just reactive and localised to the specific issue at hand—emphasis should also be placed on:

(a) the wider and potentially interconnected issues that a particular incident or set of incidents, policy breaches or near misses reveal about an organisation's internal risk profile; and/or

(b) a deep understanding of the external impact of a particular incident or set of incidents on individual market users or the market more broadly.

68 The enhancements needed are in some cases material, and are directed at:

(a) ensuring appropriate access to critical technical, process and stakeholder information in the event of an incident, through effective embedded knowledge management systems and processes;

(b) continuing to develop tool sets which allow for easy collaboration in incident response, rapid communication and scientific assessment of specific impacts or accurate performance reporting;

(c) avoiding duplicative and decentralised issue management processes and systems which cause double handling and poor capture of incident data; and

(d) avoiding internal processes which define incidents in broad terms and can contribute to inconsistent assessment and recording, across different internal teams, of issues and their impact.

69 A further challenge is the need for improved record keeping, with consistent quality and accuracy of data creation, retention and presentation across the organisation.

70 We have been concerned about ASX Group's approach to root cause analysis of incidents. The improvements to ASX Group's incident management system contained in the work plan will, once fully embedded, address our concerns.

71 It is critical that firms have the tool set required to deliver a holistic and integrated understanding of incidents, system performance and availability. ASX Group has multiple systems and decentralised processes which are

concurrently applied to manage issues. To meet industry better practice and our expectations, there should be arrangements for:

(a) effective incident impact assessment to enable automated reconciliation of the impact across affected processes, systems and stakeholders;

(b) aggregation of similar and related incidents to assist with determining impacts, sharing information between teams to improve situational awareness, and improving targeted communications to affected parties;

(c) rapid access to critical system information such as disaster recovery plans (which we identified in REP 509 as an issue for ASX Group, and which the review confirmed is still an issue);

(d) rapid and automated escalation and communication of incident information to help, where necessary, with strategic decision-making;

(e) an enterprise-wide view of each incident, its impacts and response activities; and

(f) live monitoring of team and system performance against service level and regulatory requirements.

## Recommendations

72 Table 4 sets out a summary of the steps ASX Group is focusing on to further improve its approach to incident management. ASX Group had already commenced some elements of this work prior to the review or had plans to do so. The work in Table 4 also forms part of the current ASX Group work plan that ASIC and the RBA are closely monitoring.

73 We encourage all other important financial institutions we regulate to evaluate the maturity and effectiveness of their own incident management arrangements in relation to the recommendations contained in Table 4—and to consider the application of this report's findings and recommendations in the context of their own business.

**Table 4: Steps to further improve ASX Group's incident management**

| | |
|---|---|
| **Centralise information** | Continue to develop 'whole-of-organisation' management of incidents and systems availability and develop a single source of truth with respect to IT asset criticality and system dependencies<br>Continue to aid the rapid assessment of incidents and identification of likely impacts across the organisation's operations by centralising business impact assessment processes and integrating these into the incident management software tool |
| **Service and incident management software** | Continue to implement a unified service management tool/process across all IT and operations functions, including related business units such as facilities management and business continuity, to improve incident analysis and response |

| | |
|---|---|
| **Incident management definitions and criteria** | Embed agreed incident management policies and procedures, including defined severity thresholds, near misses and customer impact, and report incidents on a consistent basis across the organisation. Review regularly to ensure the right information is captured and effectively characterises and measures severity and impact to provide meaningful strategic analysis |
| **Incident management records and guidance** | Continue to improve the accuracy, consistency and utility of incident data by identifying all required data outputs (e.g. management reporting, problem management and action tracking) and by reviewing incident classification and impact (e.g. customer impact and root cause analysis) |
| **Knowledge management** | Seek to develop greater knowledge sharing across the organisation by ensuring appropriate staff have access to critical system and process information (e.g. disaster recovery plans). Seek to limit the risk of losing intellectual property through staff departures by uploading critical information and processes into a single source of truth. Improve the utility and content creation times for key documents |
| **Crisis communication tools** | Continue to implement a rapid, mass crisis communication tool that is integrated with incident management and other critical systems. This tool should be capable of targeted and broadcast communications (e.g. via SMS); incorporate escalation management processes; and allow two-way communication, capable of integrating with the incident recording system |
| **Incident management roles and responsibilities** | Embed the operational effectiveness of responding teams across all incident domains (e.g. IT, operations, business continuity and crisis management) by rolling out the agreed enhanced roles for key common functions such as incident response coordinator and specialist incident analyst |
| **Incident management processes and policies** | Improve the consistency of incident management practices throughout the incident life cycle (i.e. from event to lessons learned), by ensuring incident management is a clearly integrated process from the point of identification/notification onwards<br>Apply consistent practices across issue tracking systems to clearly link incidents with other records (e.g. known problems, near misses and control breaches) to enable seamless escalation and early identification of emerging threats |

# G Next steps

74 ASX Group has agreed to undertake an extensive work program that incorporates all the recommendations of the review. Initial work on this program has commenced. Other work previously underway, that deals with aspects of the review's recommendations, is also being incorporated into the work program. A substantial portion of the work plan is scheduled for completion by the end of 2018. ASX Group anticipates that it will take three years to fully implement and embed this program, which it expects to be completed by December 2020.

75 An engagement plan has been agreed with ASIC and the RBA to provide oversight on the timely progress and efficacy of the work program.

76 In addition to the agreed formal engagement plan, as part of our ongoing oversight role, ASIC and the RBA will also interact with ASX Group as required to obtain detailed information on specific initiatives and to assess the impact of the program on other ASX Group initiatives and priority projects.

77 The ASX board and senior management are ultimately responsible for ensuring that ASX Group meets its statutory obligations. The board has emphasised its commitment to this work program and its accountability for delivery.

# Key terms

| Term | Meaning in this document |
|---|---|
| ASIC | Australian Securities and Investments Commission |
| ASX 24 | The licensed derivatives exchange market operated by Australian Securities Exchange Limited |
| ASX Clear | The licensed CS facility operated by ASX Clear Pty Limited (formerly known as Australian Clearing House Pty Limited) |
| ASX Clear (Futures) | The licensed CS facility operated by ASX Clear (Futures) Pty Limited (formerly known as SFE Clearing Corporation Pty Limited) |
| ASX equity market outage | On 19 September 2016, ASX experienced a hardware failure in its equities trading system, ASX Trade |
| ASX Group | The ASX group of companies including ASX Limited, ASX 24, ASX Clear, ASX Clear (Futures), ASX Settlement and Austraclear |
| ASX Limited | The licensed securities exchange market operated by ASX Limited |
| ASX Settlement | The licensed CS facility operated by ASX Settlement Pty Limited (formerly known as ASX Settlement and Transfer Corporation Pty Limited) |
| Austraclear | The licensed CS facility operated by Austraclear Limited |
| COBIT 5 | A framework for the governance and management of enterprise IT developed by ISACA |
| Corporations Act | *Corporations Act 2001*, including regulations made for the purposes of that Act |
| COSO ERM | Committee of Sponsoring Organizations of the Treadway Commission’s *Enterprise risk management—Integrated framework* |
| CS facility licensee | A clearing and settlement facility operator licensed to operate a CS facility in Australia under Pt 7.3 of the Corporations Act |
| EA | Enterprise architecture—a conceptual blueprint that defines the structure and operation of an organisation, which guides how it will execute its business and technology strategies, identify risks and achieve its current and future objectives |
| Financial Stability Standards | The RBA determined Financial Stability Standards for licensed CS facilities under s827D(1) of the Corporations Act on 10 December 2012 |

| Term | Meaning in this document |
|---|---|
| GRC system | A software tool used to manage governance, risk and compliance activities |
| ISO 31000:2018 | International Organization for Standardization's *Risk management—Guidelines* |
| ISO/IEC 38500:2015 | International Organization for Standardization's *Information technology: Governance of IT for the organisation* |
| KRI | Key risk indicator |
| market licensee | A market operator licensed to operate a market in Australia under Pt 7.2 of the Corporations Act |
| market participant | As defined in s761A of the Corporations Act |
| RBA | Reserve Bank of Australia |
| REP 509 (for example) | An ASIC report (in this example numbered 509) |
| RG 211 (for example) | An ASIC regulatory guide (in this example numbered 211) |
| s792A | A section of the Corporations Act (in this example, numbered 792A), unless otherwise specified |

# Related information

## Headnotes

ASX, clearing and settlement, Corporations Act, CS facility, default, enterprise architecture, equity market outage, financial market infrastructure, futures market, incident management, IT, licence, market operator, market participant, operational risk management, outage, post-trade, RBA, risk appetite, risk register, roadmap, securities, 19 September, technology governance.

## Regulatory guides

RG 172 *Financial markets: Domestic and overseas operators*

RG 211 *Clearing and settlement facilities: Australian and overseas operators*

## Legislation

Corporations Act, s792A(a), 792A(d), 821A(a), 821A(d)

## Reports

REP 509 *Review of the ASX equity market outage on 19 September 2016*

## Media releases

16-352MR *ASIC statement on review of ASX technical failure on 19 September 2016* (14 October 2016)

## Other publications

ASX Corporate Governance Council 2014, *Corporate governance principles and recommendations*, 3rd ed. (PDF 1.41 MB)

COSO, Enterprise risk management—Integrated framework

ISACA, COBIT 5

ISO 31000:2018 *Risk management—Guidelines*

ISO/IEC 38500:2015 *Information technology: Governance of IT for the organisation*

RBA, Financial Stability Standards for licensed CS facilities

The Open Group, The Open Group Architecture Framework

Zachman International, Zachman Framework for Enterprise Architecture