White Paper

Auditing IT Governance Structures

WP0217 | November 2015

Russel Jones

Russel Jones is an Orbus consultant with more than seven years experience in business and IT architectures, design and planning.

He has broad industry and region experience spanning financial services, natural resources and retail.

His Education and Certifications include: COBIT 5, CISA, TOGAF 8/9, ITIL 2011, Prince 2, ArchiMate 2 and B.Com Economics.

Executive Summary

IT governance ensures that the operations of IT are aligned with the requirements of the business, and as such is important in determining the return on investment gained from IT initiatives within any organization. Ensuring the IT governance structures are properly aligned to business needs and that they are delivering intended outcomes is where an IT governance audit becomes important. One vital component of this audit includes the assessment of the framework or structure of the IT governance capability. Auditing IT governance structures provides management with the assurance that the IT governance is effective and supporting the organizations strategy and objectives.

This paper will introduce the few practices and process useful for auditing IT governance structures, and references the Institute of Internal Auditors (IIA) International Standards for the Profession of Internal Auditors guidance as a baseline for the audit process.

Determine the Scope of an IT Governance Audit

There are a number of considerations to define the scope and focus of the IT governance audit. Firstly, an auditor should understand the composition of IT governance structures. The second consideration is the complexity of the IT organization being audited, as well as governance maturity.

IT governance structures consist of processes, organization structures, objectives and strategies (see previous Orbus Whitepaper Setting up Best Practice IT Governance Structures). Other components of an IT governance capability include:

- Executive leadership and support
- Service delivery and management
- Strategic and operational planning
- IT organization and risk management

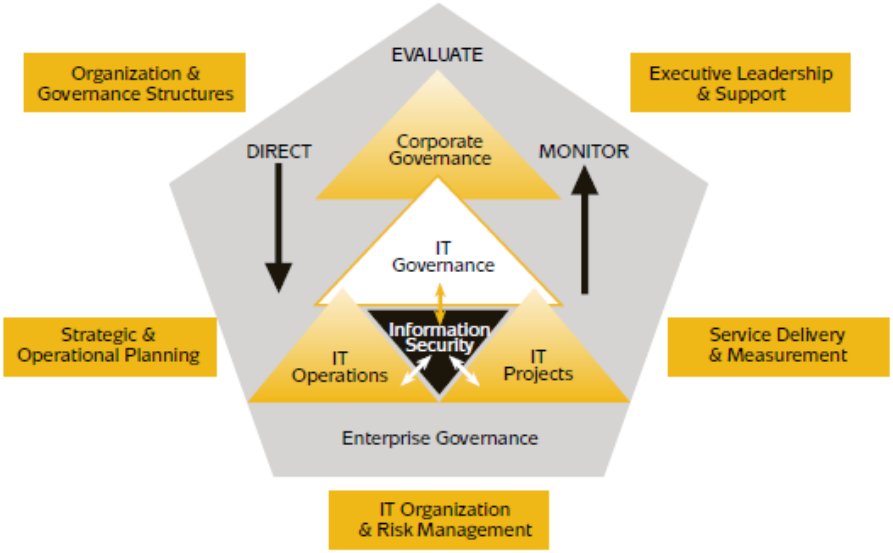

Figure 1 - IT Governance - Five Components (Source: IIA)

IT auditors can get a good understanding of IT governance maturity by targeting the following areas during an audit pre-assessment;

- Review the role of IT in the organizations strategy and mission;
- Assess the business processes with a view of determining to what degree they are automated;
- Determine the complexity of the IT landscape through assessing metrics such as the number of applications per business unit, the number of application integration points, the number of data centers, and whether IT is managed internally or supported through outsourced partners;

- Measure the level of data reuse (or duplication) and standardization across business units, applications and geographies;
- Assess whether adequate IT procurement policies are in place and being enforced;
- Investigate whether any industry best practice frameworks such as COBIT and ITIL are being used or referenced as benchmarks;
- Examine the IT risk management structures with a view of determining regulatory compliance and the existence of controls.

An understanding of these key areas of the IT organization will give the auditor a good foundation for a detailed examination of each component of the IT governance structure.

Auditing and Assessing IT Governance Structures

IT investments generally see a return over a medium to longer period than other business investments (due in part to user adoption, migration and integration costs of new technologies, etc.). The implication is that the organization's mission and vision should be well defined and communicated over the medium and long term in order for IT investment strategy to support it.

The IIA standard 2110 states the internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives. The primary goal of IT governance should be to ensure business needs and strategy are being supported by IT. As such, this should be the overarching focus when performing an IT governance audit.

There are two types of IT audits that can be carried out; performance based audits and audits of policy and regulatory compliance. Performance based audits are generally more internally focused, assessing internal structures such as processes and associated measures, the quality and existence of work products, etc. As such performance based assessments will be influenced by the maturity of the governance structures – if no processes are defined, a performance based audit will not be very useful other than to identify the gaps. Compliance focused audits on the other hand may focus on both internal policy and procedure compliance as well as compliance with external regulations and legislation. These types of assessments may be more common in regulated industries such financial services, and are less reliant on the maturity of the governance structures of the organization – either the organization is meeting the regulatory requirements or not.

According to IIA Standard 2200: Engagement Planning states that internal auditors must develop and document a plan for each

engagement, including the engagement's objectives, scope, timing, and resource allocations. This work product will form the guideline for the audit, ensuring there are clear outcomes and questions to be answered, and that scope creep is avoided. The first step from the auditor is to assess the design of the IT governance structures (in accordance with IIA 2110.A1 the internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities). In order to do this there are a number of areas to investigate;

- The IT organization structure and its integration with the rest of the organization – determining, for example, whether the CIO is a member of the executive board or senior management team.
- The change management process and how IT-related risks are identified, controlled and mitigated.
- The existence and effectiveness of governance structures, also assessing the existence of a 'feedback loop' from internal audit to governance according to IIA 2110, which states the internal audit activity must assess and make appropriate recommendations to improve the governance process.

Once the existing and maturity of the structures have been assessed, the auditor can progress to reviewing the key areas of the structure, in accordance with IIA 2110.A2 the internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives. Key considerations of this review include;

- Existence, accuracy and relevance of documentation – such as process outputs, regulatory requirements etc.;
- Existence and effectiveness of the management reporting;
- Effectiveness of risk management and mitigation processes;
- Existence, availability and relevance of strategy plans and objectives;
- Board and committee meeting minutes;
- Support for IT governance by business units and departments.

Closing Actions and Remediation

On completion of the assessment, the audit committee should provide results and feedback of the audit in-line with IIA Standard 2400; Communication Results. This standard states that the closing out communications must include the initial engagement objectives and goals of the audit, as well as any conclusions, recommendations and action plans based on the findings.

Additional considerations for communicating the audit results also include the criteria for communicating the audit results (IIA Standard 2410), and the quality of the communications (IIA Standard 2420).

Internal auditors, as part of communicating the results of the audit, are required to provide recommendations and action plans to remediate any discrepancies or findings arising from the assessment. The action plans and recommendations should be implemented as part of ongoing governance and should be the focus of subsequent audits to ensure they have been properly implemented.

Conclusion

With IT spend increasing exponentially for more and more organizations today it makes sense to ensure that well defined and mature IT governance is in place to provide management with assurance that the organization is seeing a return on this investment. Best practice frameworks such as COBIT, ITIL and others are becoming commonplace for organizations who are trying to get control of the IT organization. Defining and implementing IT governance structures based on these frameworks is the first step to ensuring compliance.

The second important activity is assessing the effectiveness of these structures, and adopting a principle of continuous improvement of governance. Luckily, well defined standards and policies for auditing governance structures have been developed by ISACA (in the COBIT publications), and by the IIA.

Bibliography

International Standards for the Professional Practice of Internal Auditing (2015), The Institute of Internal Auditors (IIA).

Available from: http://www.theiia.org/guidance/standards-and-guidance/ippf/standards/full-standards/?search=risk

[Accessed 14 November]

The Global Technology Audit Guide (GTAG): Auditing IT Governance (2012), The Institute of Internal Audits (IIA).

Available from: https://iia.org.uk/media/49473/gtag17_auditing_it_governance.pdf

[Accessed on 14 November]

IT Auditing and Controls: IT Governance and Controls Part 5 (2015), The Infosec Institute.

Available from: http://resources.infosecinstitute.com/itac-governance/

[Accessed on 14 November 2015]

COBIT 5 Implementation (2012), ISACA. Available to ISACA members from the ISACA bookstore

Available from: http://www.isaca.org/COBIT/Pages/COBIT-5-Implementation-product-page.aspx

[Accessed on 14 November 2015]

Orbus Software UK
London

Orbus Software US
New York

Orbus Software AUS
Sydney

Orbus Software RSA
Johannesburg

enquiries@orbussoftware.com | **www.orbussoftware.com**

Seattle Software Ltd. Victoria House, 50-58 Victoria Road, Farnborough, Hampshire, GU14 7PG. T/A Orbus Software. Registered in England and Wales 5196435