Vision for IT Audit 2020

Berthing, Hans Henrik

Publication date:
2014

Document Version
Early version, also known as pre-print

Verifica

Vision for IT Audit 2020

Partner Hans Henrik Berthing,
Statsautoriseret Revisor, CIA, CGEIT, CRISC, CISA

Agenda

- Challenges for IT Auditors today

- Cloud Governance
- Third party reporting ISAE 3402/3000
- Cybersecurity
- Talent management
- Knowledge and research

- COBIT 5 and COBIT 5 Online

Hans Henrik Berthing

- Married with Louise and dad for Dagmar and Johannes
- CPA, CRISC, CGEIT, CISA and CIA
- ISO 9000 Lead Auditor
- Partner and owner for Verifica
- Financial Audit, since 1994 and IT Assurance since 1996
- Member of FSR IT Advisory Board
- ISACA IT Assurance Task Force
- Cobit 5 Online Beta tester
- Instructor, facilitator and speaker
- Senior Advisor & Associated professor Aalborg University (Auditing, Risk & Compliance)

Challenges facing IT auditors today

- Resource (i.e., budget, staff) Issues
- Technology, Tools & Aids
- Auditee/Organizational Issues
- IT Compliance

Resource (i.e., budget, staff) Issues

- Attracting right talent /Availability of experienced auditors
- Professional development and study of new technologies and techniques
- Invited to the table strategic and tactical directions.
- Developing the soft skill-set expected of all auditors.
- Education of IT auditors
- Gap between IT skills and auditing skills
- Have the necessary budgets to carry out the function
- Better salaries and career development in the operation areas.
- Lack of technical knowledge
- Low interest at educational institutions (Universities)
- Multiple IT standards -> more budget/manpower/time
- Audit Report which has industry specific business language
- Staying current with rules and regulations
- Understanding business strategies (non-technical)

Technology, Tools & Aids Issues

- IT Audit frequency + scope aligned with frequent technology update changes.
- Effective risk assessment / Scoping relevant systems
- Heavy adoption of IT by Organizations resulting in Multiple applications
- Ability to align scope and results with business strategy and risks
- Clarifying how business risk can be better mitigated with IT controls
- Addressing the risks associated with Cloud computing technology
- Keeping on top of regulations by industry
- Add a new level of innovation to review processes
- Audit standardization / Automated controls testing/ Availability of audit tools
- Controls Identification and its Testing
- Existence of technological continuity plans to ensure business continuity.
- Having a good mix of audit and security tools
- Defining observation major, minor or level of risk identified
- Legacy differentiation between Data Privacy and Information Security
- Use of third party providers

Auditee/Organizational Issues

- Business Acceptance/Having support of senior management
- Growing number of persons who rely on the opinion of auditors
- IT audit is perceived to add less value at Strategic and Governance levels.
- Lack of credibility by the auditee to the work of the auditor
- Little documentation of the work performed by the audited
- Proving business value in audit as to just compliance
- Delay on delivery of Information by the auditee
- Difficult acceptance of the observations made by audited areas
- Educating on the importance of IT procedures in relation to the overall audit
- Gap between the Financial Reporting and the IT auditors
- Having a hierarchical level within the organization that allows direct access to senior levels
- Increased complexity of the organizational environment
- Cost cutting leading to non-prioritization of Infosec issues mitigation
- Inexperience of client with their own technology

IT Compliance

- IT-compliance-related effort expected to increase without significant changes to staff count
- IT compliance budgets are estimated to increase (7-10% of IT budget to compliance)
- Internal IT audit teams spend an estimated 17.5% of their time on IT compliance and privacy each, 20% each on information security and IT risk management, respectively, and about 15% on business continuity management

Current state -> Plan 2020

- Cloud Computing
- Service organisation
- Cybersecurity
- Talent management
- Knowledge and research
- COBIT 5 Online

Cloud computing

Business Benefits of Cloud Computing

- Cloud strategies make the enterprise more efficient and agile.
- Cloud computing allows delivered services to be more innovative and more competitive.
- Cloud computing reduces overall operating costs.

- How confident can boards be that management plans will achieve these benefits?

Source: CLOUD GOVERNANCE: Questions Boards of Directors Need to Ask, 2013, ISACA

Value of Cloud Computing

- Shifting funding of IT from large capital investments (legacy IT assets) to operational expenses.
- Reallocating IT resources to core business activities.
- Easier and cheaper applications to implement, use and support.
- Increasing scalability and flexibility, enhancing the ability to respond to changing market conditions.
- Fostering innovation by shifting effort and resources from implementation projects to final product development.

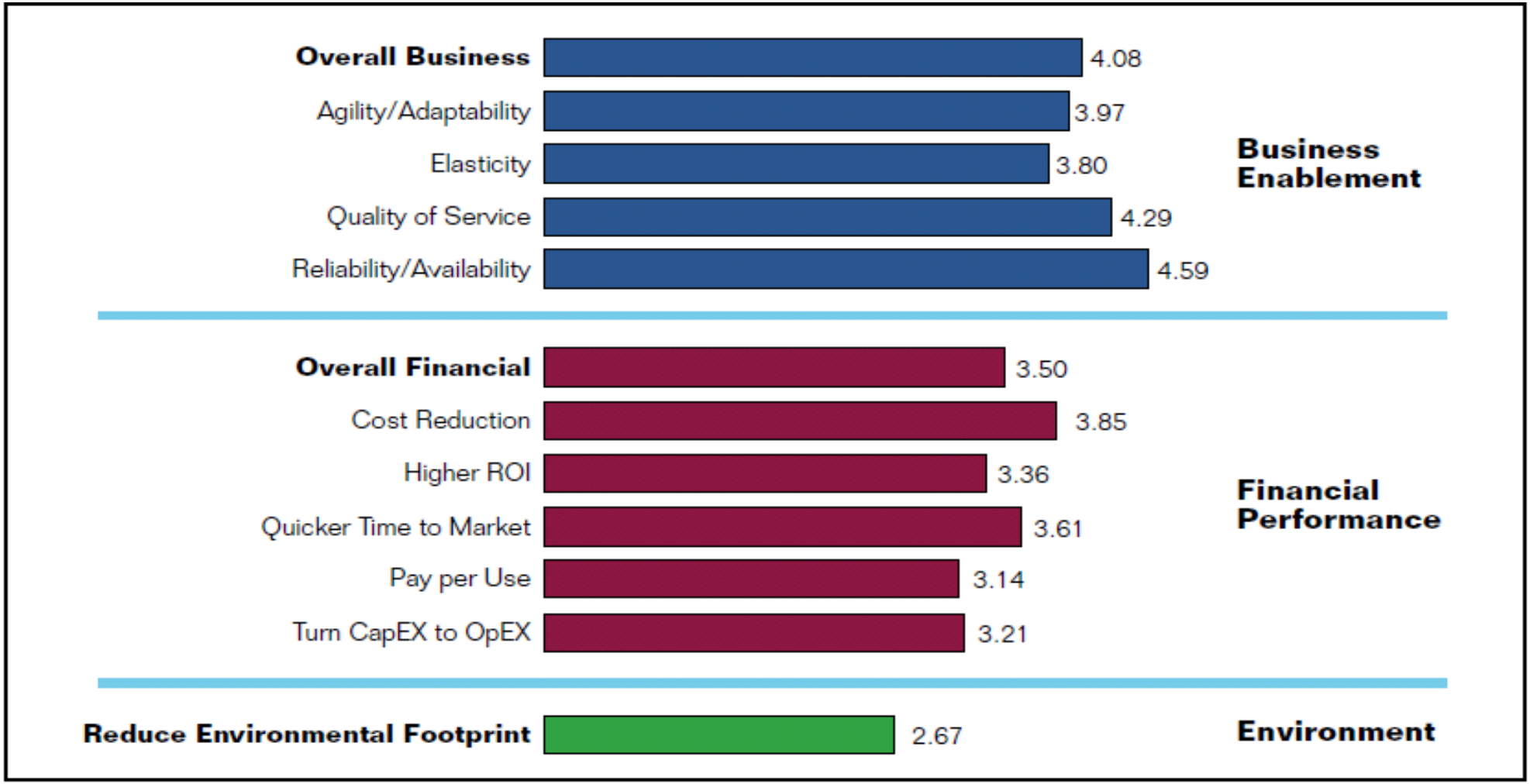
Source: CLOUD GOVERNANCE: Questions Boards of Directors Need to Ask, 2013, ISACA

Governance Questions About Cloud

1. Do management teams have a plan for cloud computing? Have they weighed value and opportunity costs?
2. How do current cloud plans support the enterprise's mission?
3. Have executive teams systematically evaluated organizational readiness?
4. Have management teams considered what existing investments might be lost in their cloud planning?
5. Do management teams have strategies to measure and track the value of cloud return vs. risk?

Source: CLOUD GOVERNANCE: Questions Boards of Directors Need to Ask, 2013, ISACA

Cloud Decisions



Source: Cloud Computing Market Maturity *Study Results, 2012, ISACA & CSA*

Cloud computing plan? (n=914)

	We do not use it for any IT services.	We use it for low-risk, nonmission-critical services.	We use it for mission-critical services	Unsure
Public cloud	**63%**	22%	3%	12%
Private cloud	**34%**	27%	26%	13%
Hybrid cloud	**55%**	15%	4%	26%

Source: IT Risk/Reward Barometer: Europe, 2012, ISACA (n=980)

Risks and Security Concerns With Cloud Computing

- Reputation, history and sustainability of the provider
- Failure to perform to agreed-upon service levels
- Where information actually resides
- Third-party access to sensitive information
- Compliance to regulations and laws in different geographic regions (Public Clouds)
- Information may not be immediately located

Source: Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives, 2009, ISACA

Assurance Considerations

Transparency

Privacy

Compliance

Trans-border information flow

Certification

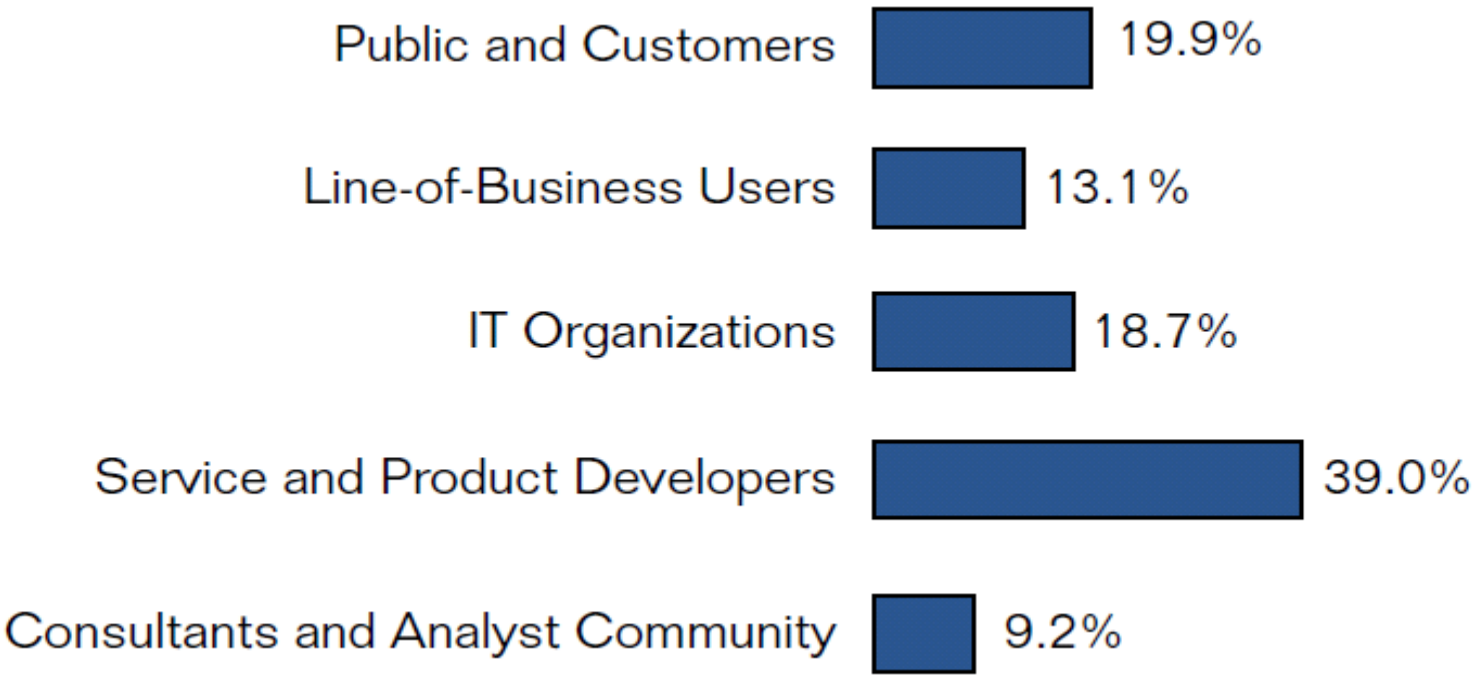
Source: Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives, 2009, ISACA

Cloud Market Maturity

Table 1—Cloud Market Maturity Model	
Stage	**Distinguishing Elements of the Cloud Market**
Infancy	The market is small with a potential for growth and innovation that has not been realized. The definition of cloud and related roles and responsibilities is not clear. ROI is uncertain. Users and providers can be considered early adopters.
Growth	The market demonstrates significant adoption, rapid growth, and notable innovation in terms of product offerings and use. Definitions of cloud computing and how it can be leveraged are clear. Roles and responsibilities for cloud within the enterprise have evolved to address cloud's unique aspects. Could computing is being integrated into core business activities. ROI is clear and examples of successful use are well known. Innovation leads to new product offerings not possible in earlier stages.
Maturity	Market growth has reached its peak. The level of innovation is slowing. New entrants have a difficult time distinguishing themselves from established service providers. Organizational roles and responsibilities are stable, as are relations between users and providers. Cloud computing is business as usual.
Decline	The cloud market is saturated with suppliers. Cloud computing is a commodity. Market leaders are clearly defined. There is little room for new entrants or new product offerings. Users and providers are looking for the next big opportunity.

Source: Cloud Computing Market Maturity *Study Results, 2012, ISACA & CSA*

Groups Driving Cloud Innovation



Source: Cloud Computing Market Maturity *Study Results, 2012, ISACA & CSA*

Cloud Support for Business Goals

Goal	Rank	Mean Score
Experiment with new technologies	1	3.58
Provide new services to enhance worker effectiveness and efficiency	1	3.58
Experiment with new ways of engaging with customers	2	3.53
Take new ideas to market	3	3.43
Provide access to best-in-class tools and capabilities	4	3.25

Source: Cloud Computing Market Maturity *Study Results, 2012, ISACA & CSA*

Service audit reports

Many business events have altered the landscape since the issuance of Service Audit Reports

- Increased outsourcing including usage of shared service centers
- Continued globalization and global processing models
- Increased regulation and enhanced risk management requiring service organization customers to obtain controls comfort related to outsourced activities impacting their financial statements, regulatory requirements and overall business risk management
- Other territories have steadily sought to adopt their own service
- Absence of a global standard(s) complicates engagements that cross borders
- Potential to take advantage of differing provisions within various third party control standards

Perspective of the User Entity

- Regulatory requirement
- The board of directors focusing on corporate governance,

  Design and implementation of internal control over financial reporting have become key responsibilities for management.

- Trend for strong internal control
- Continuing trend to outsource functions that may be significant to an organization's operations.

  Enterprises transferred performance of many of their key controls to third-party service organizations.

  Controls can be outsourced but management's responsibility for maintaining an effective system of internal control cannot be outsourced.

Complementary user entity controls

An ISAE 3402/3000 audit report identifies the controls designed to achieve the control objectives, including potential controls that the service organization intends for the user entity to implement (referred to as "complementary user entity controls").

While the specified controls should address the risks that threaten the achievement of the control objective for most user entities, individual user entity needs may vary.

As a result, user entities should consider the risks that would threaten the achievement of the control objectives from the perspective of the user entities and consider whether the controls identified adequately address those risks.

If the user entity believes that any risks are not addressed by the service organization's controls, the user entity should discuss those risks with the service organization.

Service organization responsibilities

Service organizations have five primary responsibilities:

1. Prepare and present a complete an accurate description of the system
2. Specify the control objectives of the system and state those control objectives in the description of the system
3. Identify the risks that threaten the achievement of the control objectives (although these risks are not included in the service organization report)
4. Design, implement and maintain controls to provide reasonable assurance that the control objectives will be achieved
5. Provide a written assertion to accompany the description as to the completeness and accuracy of the information provided and state the criteria used as a basis for making the assertion

Subservice organizations

- A subservicer is a service organization used by another service organization
- "Carve-out" or "inclusive" methods are available for dealing with services provided by subservice organizations in the report.
- Identify all subservice organizations that affect user entities' financial statements.
- Does subservice organizations have existing service organization reports or would be willing to provide one to your customers. (Cheaper and easier to provide your customers with a copy and limit your report to only your processes).
- Discuss reporting strategy with subservice organization.
- Assistance and cooperation with the subservice organization
- Obtain agreement with your subservice organization regarding strategy, and get this agreement in writing.
- If you are a subservice organization, discuss with the primary service organization how the needs of their clients will be met.

Privacy – ISAE 3000

- Compliance with data protection act
- ”Databehandleraftale”
- Third party reporting – ISAE 3000
- ISO 27001 or ISO 27002
- Type 2
- Description of controls and IT auditors test of controls
- Period covered
- Subservice organisation
- Complimentary Controls

Cybersecurity

- Cybercrimes and violations are growing exponentially
- Organizations suffer a sort of inertia in having a pro-active policy of cyber audits and other such initiatives.
- Lack of reporting and sharing cyber incidents and their after effects with the community
- Audits will make organizations aware and pro-active in cyber security.
- COBIT 5 for Cybersecurity

Talent management

Certifications

- Improve and marketing CISA
- Advanced-level
- IT Audit Foundation

Courses

- Leadership in IT Audit
- Focus for senior IT professionals.
- Audit Ethics
- Effective Report Writing
- Soft skills
- Financial Foundation

Career path for IT Auditor

Knowledge and Research

- Common IT findings/compensating controls.
- Practical guidance on ISAE3402/3000.
- Guidance on generic application controls
- Emerging technologies
- Using COBIT 5
- Audit Handbook for beginners

COBIT 5 – COBIT 5 Online

1. Increase awareness of COBIT 5 across a broader audience of stakeholders who are responsible and accountable for the success of IT-enabled investments.
2. Increase the perceived relevance of COBIT 5 as a business framework for ensuring the success of IT-enabled investments, from inception through to adoption, management and governance.
3. Increase the utility of COBIT 5 by making it easier for users to understand, customize, socialize and deploy; and to help facilitate greater adoption of COBIT 5 among enterprise stakeholders.

Summary

- IT Auditors have lots of challenging
- Resources
- Knowledge
- Career management
- Risk mitigation/management
- Cloud Computing
- Third party reporting
- Soft skills

- COBIT 5 Online – a nice tool for the IT Auditor

Questions

Hans Henrik Berthing, Statsautoriseret revisor

| CGEIT | CRISC | CISA | CIA

Phone +45 35 36 33 56 |

Mobile +45 22 20 28 21 |

E-mail hhberthing@verifica.dk

Verifica

Statsautoriseret Revisionsvirksomhed