

Advanced Module A1

SABSA Risk, Assurance & Governance Master Class

Risk Management

All business, whether it be commercial, government, military or charitable, is based upon exploiting opportunities to further the goals of the enterprise. With each opportunity comes risk, and thus risk is implicit in doing business, whatever the nature of that business. To do business is to take risks.

Risk management is the art and science of managing business risks in such a way as to match the risk tolerance (or risk appetite) of the enterprise. This means that all risks must be identified, analysed, assessed (measured) and perhaps mitigated to ensure that they are within the risk appetite and that the overall costs and benefits associated with managing the risks are optimised.

There are several important concepts relating to the complexity of risk management. Firstly, risk cannot be avoided. For any planned business activity or action there is a risk associated with taking that course of action and a risk associated with not doing so. 'Doing nothing' does not avoid risk. Secondly, although it is convenient to organise risks into categories and groups for identification and analysis purposes, risks do not actually behave in a silo manner. Risks affect one another in a complex web of interactions, such that mitigating or reducing a given risk may well increase one or more other risks. Thirdly, risks at the micro-level of the enterprise may or may not be significant at the macro-level, and thus risk aggregation and scaling techniques are necessary as part of the overall risk management strategy.

To summarise, risk is implicit in doing business of any kind, and is the flip side of business opportunity. Thus risk management is synonymous with business management. Every business decision is a risk decision. Hence, all organisations take risk. The most successful are those that consistently make the best risk management decisions. Good management decisions are dependent upon high-quality information and a superior framework within which to present that information to exercise good judgement, reach the best conclusions and provide workable solutions to new problems. SABSA provides such a framework.

Assurance Management

Not only does an organisation need to plan and execute an appropriate information security and risk management programme – the senior management team also needs to have a means by which it can check that this is so – to

provide assurance that all is well in this respect. Assurance management is the activity that provides this feedback on the quality and completeness of the information security and risk management programme. Assurance management is an integral part of the SABSA framework, within which the business receives assurance that all of the Business Attributes in the SABSA Business Attributes Profile are being provided to a level compatible with the performance targets that have been set for each one.

Risk and Security Governance

The SABSA Framework provides its own security and risk management governance framework for ensuring that all aspects are in line with the strategic direction set by the senior management.

Course Overview

This five-day intensive SABSA Risk, Assurance and Governance course module and workshops empowers anyone involved with governing, managing, measuring and mitigating enterprise risk and assurance to meet their obligations through a framework and proven techniques that enable excellence in enterprise decision making.

The course provides participants with a practical guide on how to govern and manage risk and assurance levels within their business operations. It covers general Operational Risk Management concepts with a consistent and practical focus on the specific needs for managing risk in the wider context of a SABSA-based enterprise information security architecture and risk management programme.

High-Level Learning Objectives

After attending this course a course attendee will be able to:

- Plan, develop, implement and manage a strategic enterprise-wide operational risk management framework, methodology, tool-set and process, aligned to the SABSA framework
- Plan, develop, implement and manage an information assurance and information risk management strategy and programme within the SABSA framework
- Implement a SABSA-based IT and information security governance framework within which to develop information security, information assurance and information risk management policies

- Define business-driven SABSA control objectives and enablement objectives and manage projects
- Apply SABSA operational risk management techniques and methods in the context of information risk and information assurance
- Apply the SABSA operational risk management and information assurance techniques and methods both at the enterprise-wide level and at the project level
- Develop an over-arching SABSA Enterprise Risk Management strategy to address the issues of isolated risk silos and create an integrated, holistic approach
- Discover, analyse and evaluate internal and external business factors, including regulatory regimes, to drive the priorities of the SABSA business risk strategy
- Develop practical SABSA methods to measure risk, set performance targets for risk appetite and monitor actual performance against these targets
- Plan and conduct risk-based information security reviews, information security audits and implement a risk-based security audit programme within the SABSA framework
- Plan, develop, implement and manage a SABSA communications strategy and a strategic information-management architecture for capturing, transforming, processing and reporting risk information
- Evaluate alternative SABSA strategies and solutions, and make recommendations in support of decision-making by key stakeholders in terms that ensure added business value, leading to senior management buy-in and support

Design, implement and manage a business process assurance programme within the SABSA framework

- Apply capability maturity modelling techniques to plan, implement and manage a programme of continuous process and systems analysis and improvement within the SABSA framework
- Apply the SABSA framework to assure compliance with external standards such as the ISO/IEC 27000 series
- Within the SABSA framework, plan and implement a comprehensive programme for testing of systems and software to provide assurance of their compliance with business and operational requirements

Pre-Requisite Knowledge

There are no pre-requisites for attending this course or for sitting the SABSA Institute A1 examinations on completion of the course. However, attendees will probably benefit most if they have some previous knowledge of the SABSA framework, and for those wishing to be awarded the SABSA Chartered Practitioner Certificate or the SABSA Chartered Master Certificate, they will need to complete the SABSA Chartered Foundation Certificate before the Practitioner award can be made, which in turn is a pre-requisite for award of the Master certificate..

What a Course Attendee will take away

- A comprehensive knowledge of the principles and practice of operational risk management, assurance and governance within the SABSA framework
- A plan for implementing risk management and assurance management throughout the enterprise using the unique SABSA Business Attributes Profile approach combined with the comprehensive SABSA framework for risk modelling, assessment, analysis, mitigation, management and measurement.
- A new and more comprehensive definition of “best-practice” risk assessment methods that exceed existing standards and definitions through the application of the SABSA Business Attributes Profile as a proxy for the ‘assets’ at risk.
- A practical SABSA-based approach to building an ever more accurate and assured enterprise risk profile – and facilitating risk assessment of new ventures through the work already done and the lessons already learned in developing that profile.
- A plan for implementing ongoing improvement of operational risk management and assurance management through monitoring, measurement and benchmarking.

Who Should Attend

- CIO / CISO / CRO / CIRO
- IT Strategists and Planners
- IT Architects
- IT Development Managers and Project Leaders
- Software Managers and Architects

- Network Managers and Architects
- Computer / Application / Web / Network / Information Security Managers, Advisors, Consultants & Practitioners
- IT Line Managers
- IT Service Delivery Managers
- Risk Managers
- Internal and External Auditors

Methodology

The course consists of lectures and workshop sessions, supplemented by case studies drawn from a combination of published real life examples and/or practical experience. In the workshops attendees will work in small groups to synthesise ideas and strategies and to apply the material in the context of case studies and simulations. Open forum discussions will also feature where appropriate.

Lecture content is naturally less intense than in Foundation classes, with more emphasis on practical work. The course focuses heavily on developing the skills and knowledge for a practitioner or master through hands-on workshop sessions and discussions, so as to provide the appropriate balance and emphasis on practice rather than theory.

Course Outline

1. The meaning of risk, assurance and governance within the SABSA framework
2. SABSA Risk management and corporate governance
3. SABSA Enterprise risk management
4. SABSA Risk Context, Stakeholders, Business Drivers & Structure
5. SABSA Risk measurement and risk assessment
6. SABSA Risk mitigation and business enablement
7. SABSA Risk appetite and risk tolerance
8. SABSA Risk management tools
9. SABSA Risk financing
10. The Meaning of SABSA Assurance
11. SABSA Assurance Services & Techniques
12. SABSA Asset Assurance



SABSA – Advanced Module A1

13. SABSA Risk Management Assurance
14. SABSA Process Assurance
15. SABSA People Assurance
16. SABSA Location Assurance
17. SABSA Timeliness Assurance

