



Business Solutions for Africa

K-Ninety East Africa Limited
 Kenya Institute for the Blind Complex,
 Mai Mahiu Road off Langata Road
 P.O. Box 3894 GPO 00100
 Nairobi, Kenya

Tel: +254 20 608 316
 +254 20 354 4352
 Cell +254 722 771 478
 Fax: +254 20 608 318
 Email: info@k-90ea.com

IS AUDIT RISK & SECURITY COURSE (28 CPE HOURS)

<p>DAY ONE: Audit, Risk & Security Planning the IT Audit</p> <ul style="list-style-type: none"> ▪ Risk-based auditing ▪ Integrated audit approaches ▪ Developing the audit strategy ▪ Planning and executing the audit <p>Risk Assessment</p> <ul style="list-style-type: none"> ▪ Risk definition ▪ Identifying risk factors, vulnerabilities, and threats ▪ Business and technical risks ▪ Cost/risk evaluation ▪ Risk assessment factors ▪ IT risks in an automated environment <p>Introduction to ISO17799</p> <ul style="list-style-type: none"> ▪ BS7799 Origin & development; a brief introduction to explain why a British Standard became internationally recognized as the primary driver for information security ▪ Achieving ISO status; this did not just happen, but was a planned and managed project which is still ongoing ▪ ISO27001 components; where Part 1 (ISO17799) is guidelines, Part 2 is the specification on which the next part of this course is based, This will be a look through the key components of the Standard as it should be implemented. <p>Auditing Security using ISO27001</p> <ul style="list-style-type: none"> ▪ The Gap Analysis using "Annex A"; comparing where are we now with where do we want to be is a standard project exercise but this relates it directly to identifying and meeting the Business need for security and confidentiality of information ▪ The Compliance Project; where next after the Gap Analysis? Security implementation requires some special treatment as an essential part of your IT Governance project ▪ Measuring compliance; security metrics can be complicated yet the degree to which you are achieving your objectives needs to be measured and reported <p>System Software</p> <ul style="list-style-type: none"> ▪ Software integrity ▪ Operating system risks and controls ▪ Controlling privileged access ▪ Activity logging ▪ Vendor patch management ▪ Database management risks and controls ▪ Utility programmes <p>Logical Access Controls</p> <ul style="list-style-type: none"> ▪ Logical access control objectives ▪ Integrated roles of IT and business process owners ▪ Authentication objectives: password controls, tokens, and biometrics ▪ Authorisation ▪ Audit trails ▪ Managing user accounts ▪ Security monitoring ▪ Single sign-on (SSO) authentication ▪ Remote access ▪ Sensitive data on PCs and workstations ▪ Social engineering risks ▪ Centralised vs. decentralised control ▪ Access control best practices <p>DAY TWO: Audit, Risk & Security Physical and Environmental Controls Physical security objectives, risks, exposures, and controls</p>	<ul style="list-style-type: none"> ▪ Environmental exposures and risks ▪ Environmental controls: fire protection, water protection, and power conditioning <p>Network Perimeter Security</p> <ul style="list-style-type: none"> ▪ Network security threat/risk analysis ▪ Network security strategy ▪ Firewalls ▪ DMZ ▪ Intrusion detection systems ▪ Remote access ▪ Wireless access <p>Encryption</p> <ul style="list-style-type: none"> ▪ Types of encryption ▪ Symmetric and asymmetric encryption ▪ Public key infrastructure ▪ Network encryption layers ▪ Secure sockets layer ▪ Digital signatures <p>DAY THREE CobiT & ITIL Service Delivery Why IT Governance?</p> <ul style="list-style-type: none"> ▪ The case for IT and Corporate Governance; a look at some of the major issues which have 'shaken the world' and the legislation that has directly resulted from highly-publicised business failures, including Sarbanes-Oxley in the USA and beyond ▪ Executive Management in the Global Enterprise; responsibilities of executive management is being polarized by the recognized need for Corporate Governance. IT Governance is a key sub-set of this. <p>Introduction to CobiT</p> <ul style="list-style-type: none"> ▪ Summary of CobiT History & Origins; a brief look at where CobiT came from to show why it is the globally respected framework for Governance ▪ CobiT's component parts; different sections for different individuals, from the Executive to the Implementation Team ▪ CobiT, ITIL & ISO27001; an overview of the relationship between key elements of the CobiT framework and the specific tools for adding the 'meat' onto CobiT's 'bones'. <p>Introduction to ITIL Service Delivery</p> <ul style="list-style-type: none"> ▪ The IT Infrastructure Library; where ITIL came from and how it, in its own right, has become a global vehicle for delivering the IT service. ▪ The Benefits of Service Management; why ITIL is so useful in any IT environment and can be used as an audit tool <p>Service Level Management</p> <ul style="list-style-type: none"> ▪ The importance of SLA's to the IT Department; internal service level agreements focus the mind of IT on the provision of a "quality product" to meet the needs of Business ▪ Planning & Implementing the Process; "it's all in the planning" goes for any major project but with managing SLA's it has a very special meaning, especially in Governance ▪ CobiT statements as they relate to SLA's; how managing service levels fits into the CobiT Governance Framework. <p>Financial Management</p> <ul style="list-style-type: none"> ▪ What does it mean to an IT Department? Finance & IT is not always a 'hand in glove' relationship; perhaps it should be? Is IT a 'black hole' into which the business pours money? 	<ul style="list-style-type: none"> ▪ Developing an IT Accounting system; helping IT to demonstrate its value to the business and helping everyone from the executives to the everyday user to understand IT costs ▪ CobiT statements; fitting financial management into Governance <p>Capacity Management</p> <ul style="list-style-type: none"> ▪ Why (not how!); capacity management is a technical issue best left to the experts, but as a part of the IT Governance framework it is essential and must be managed as such ▪ Typical activities in capacity management; not the technical but the administration, making sure business objectives are achieved not just today, but in the future. ▪ CobiT Statements; again, fitting capacity management into your IT Governance <p>DAY FOUR CobiT & ITIL Service Support Service Continuity</p> <ul style="list-style-type: none"> ▪ Typical risks to IT Services; most businesses are dependent upon their IT services being there when they are needed. This is a look at common reasons why they might not be and how a variety of 'disruptive incidents' can be addressed ▪ Considering the scope: risks 'in' and 'out'; continuity issues need to be addressed according to business risk as addressing them can be an expensive experience! ▪ CobiT Statements; still fitting system availability as a key Governance issue <p>Introduction to ITIL Service Support</p> <ul style="list-style-type: none"> ▪ The Benefits of Service Support; why ITIL Part 2 is equally useful in any IT environment and can be used as an audit tool <p>THE SERVICE/HELP DESK</p> <ul style="list-style-type: none"> ▪ Keeping the Customer satisfied: providing the service to Business and maintaining IT as a key Business support ▪ Service Desk Technology: what is needed in the computerized service desk environment ▪ Service desk responsibilities & functions: what the Service Desk should do and what it should not do. <p>Problem & Incident Management</p> <ul style="list-style-type: none"> ▪ What is an incident? When does it become a "Problem"? When does it become a "Crisis"? ▪ Proactive Problem Management; recognizing, dealing with and managing incidents ▪ Encouraging Incident Awareness: relating ITIL to ISO27001 <p>Change, Release & Configuration Management</p> <ul style="list-style-type: none"> ▪ Identifying the risks to IT governance in changes to the IT environment: dealing with special risks including Fraud ▪ The Change Cycle: from the first ideas to the implementation of both Hardware & Software ▪ Implementing Change Governance throughout the Cycle; some ideas for the management process <p>Auditing using CobiT, ITIL & ISO27001</p> <ul style="list-style-type: none"> ▪ Risk assessment ▪ Planning the audit ▪ Developing audit programmes ▪ Testing controls ▪ Using CAATs and data analysis ▪ Workpapers ▪ Audit report ▪ Follow-up <p>Summary & Conclusions</p>
--	---	--



Business Solutions for Africa

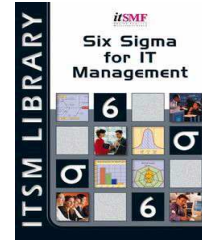
K-Ninety East Africa Limited
Kenya Institute for the Blind Complex,
Mai Mahiu Road off Langata Road
P.O. Box 3894 GPO 00100
Nairobi, Kenya

Tel: +254 20 608 316
+254 20 354 4352
Cell +254 722 771 478
Fax: +254 20 608 318
Email: info@k-90ea.com

IS AUDIT RISK & SECURITY COURSE (28 CPE HOURS)

Presenter:

**Rajeev Andharia PMP, CISA, CISSP, ITIL V3 Expert,
Six Sigma (GreenBelt)
Practitioner and Trainer – IT Service & Project
Management
Co-Author of the Book "Six Sigma for IT
Management"**



- ✓ **15 Years** in Project Management & Consulting with organizations like **Sun Microsystems, Wipro, Sify** and **L&T**
- ✓ Regularly Conducts corporate trainings on ITIL (**Foundation & Manager**), Project Management (**PMP Preparation & MS Project**) & IS Audit
- ✓ Rajeev has managed, architected and implemented comprehensive information assurance projects and managed internal, external, and contracted/outsourced information technology audits to ensure various regulatory compliance for various esteemed companies
- ✓ **Qualifications & Certifications**
 - MBA (Telecom Management) from Symbiosis, Pune
 - Project Management Professional (**PMP**)
 - Certified Information Systems Auditor (**CISA**)
 - Certified Information Systems Security Professional (**CISSP**)
 - ITILv2 Service Manager Certified
 - ITIL v3 Expert Certified
 - Six Sigma Green Belt Certified
- ✓ Co-Author of ITSM library book "**Six Sigma for IT Management**" published by itSMF, Netherland.
- ✓ Implemented solutions and consulted clients on IT governance, Service Management, Process Improvement, Information Strategy, Information Risk Management (IRM) and e-business solutions.
- ✓ Part of the team that established the first licensed PKI Certification Authority (CA) for Digital Signatures in India using Verisign Managed PKI solution.
- ✓ Successfully **managed large domestic & international Projects** in the areas of
 - Service Excellence (using best practices and standards like ITIL, COBIT, ISO 20000 and ISO 27001)
 - Information Systems Strategy / Feasibility Study / Road Maps / Architecture
 - e-business applications (Internet Banking, Supply Chain, e-commerce)
 - Information Security (PKI, ISO 27001)
- ✓ Performance driven, with a bias towards action and result-orientation, he believes in creating value for client organizations by delivering innovative business solutions.
- ✓ Exposure to Frameworks, Methodologies & Tools like OPM3, PMBOK, COBIT, ITIL, ISO 20000, ISO 27001, PKI, MOF, UML, FCAPS, Balanced Scorecards, Six Sigma.

CONTACT Loise Ngugi

K-Ninety East Africa Ltd.
P.O. Box 3894-00100
Nairobi Kenya
Tel: +254 (0)20 608316 or +254 (0)20 3544352
Cell: +254 (0)722 771478
Email: training@k-90ea.com
Web: www.k-90ea.com