Sub Committee for Curriculum Development
Information Security ManagementSpecialization

Format to submit syllabus

Course Name: Governance, Risk and Compliance

Course Code: T3035

(UG/PG): PG

Number of Credits: 2

Level: 5

Learning Objective(s): To evaluate the IT Governance and methodologies particularly in view of strategic alignment of IT with the business
To understand the standards and compliances currently available in the marketplace
Provide high level overview of several key areas of Governance, Risk and Compliance
Discuss the role of Internal Audit related to all key areas

Pedagogy:

Lectures
Lectures discussion
Seminars

Pre-learning:

Basic knowledge of businesses, Role of IT Systems; some knowledge of PM, ITIL and IT Service Management or IT audit.

Course Outline:

Sr.No.	Topic	Hours
1	Overview Introduction to Enterprise GRC, What is IT Governance, Its role in Corporate Governance, Business and importance of information technology (IT) systems, IT systems performance and risk management, Current global business scenario and the need of compliances such as Sarbanes-Oxley (USA) and Basel II (Europe)	3
2	Foundation of IT Governance Need of IT/Corporate Governance Policy, Key IT Resources and Functions to be managed, IT Governance – Organization/People, Process and Technology, Results of ineffective ITG and Methodology	3
3	Other related systems Business Service Management, Business Technology Optimization, Enterprise architecture, IT asset management, IT portfolio management, IT security assessment, IT service management, Project governance (Project management and Program management in the enterprise IT context)	3
4	Other Frameworks Introduction to IT Infrastructure Library (ITIL),Control Objectives for Information and related Technology (COBIT),ISO/IEC 27001 (ISO 27001), Information Security Management Maturity Model(ISM3) AS8015-2005, IT security (BS7799), Capability Maturity Model (CMM) Non-IT specific frameworks: Balanced Scorecard (BSC) – methods to process performance. Six Sigma – for quality assurance	3
5	Compliance Motivation, Challenges, Success Factors	1.5
6	ISO 27001 History of the standard, Key Control Areas, The PDCA model (The Plan Phase, The Do Phase, The Check Phase and The Act Phase), ISO 27001 Implementation, ISO 27001 Certification	1.5
7	COBIT Overview of the Framework, IT Governance Focus Areas, Need for a Control Framework, COBIT Information Criteria, Business Goals and IT Goals, IT Resources, Four Domains of COBIT, IT General Controls and Application Controls	3
8	HIPPA The Law and DHHS, HIPAA Regulations and Standards (The Privacy Rule, HIPAA Statute, The Security Rule, Transactions and Code Set Standards, Identifier Standards), Compliance and Enforcement	3

9	SOX Section 302, Section 404, Application	3
10	BASEL-II Need for Basel, 3 Pillars concept, Application	3
11	California SB 1386 and AB 1950, UK Data Protection Act, Australian Privacy Act Overview of each Legislation, Need, Current Status	3
	Total	**30**

Books Recommended:

1. The Governance, Risk, and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices by Anthony Tarantino
2. Enterprise Governance of Information Technology: Achieving Strategic Alignment and Value by Wim Van Grembergen, Steven De Haes, Springer, 2009
3. Implementing Information Technology Governance: Models, Practices and Cases by Wim Van Grembergen, Steven De Haes, IGI Publishing, 2007
4. IT Governance: How top performers manage IT decision rights for superior results by Peter Weill and Jeanne W. Ross; Harvard Business School Press, 2004
5. IT Savvy: What Top Executives Must Know to Go from Pain to Gain by Peter Weill, Jeanne W. Ross, Harvard Business Press, 2009
6. Enterprise architecture as strategy: creating a foundation for business execution By Jeanne W. Ross, Peter Weill, David Robertson, Harvard Business Press, 2006

SOA Governance: Achieving and Sustaining Business and IT Agility by William A. Brown, Robert Laird, Clive Gee and Tilak Mitra, IBM Press, 2008

8. CISA Review Manual 2011 By Isaca
9. IT Governance based on Cobit 4.1 - A Management Guide (ITSM Library), Van Haren Publishing; 3rd edition
10. IT Governance: A Manager's Guide to Data Security and ISO 27001 / ISO 27002 by Alan Calder, Steve Watkins, Kogan Page, 2008
11. Sarbanes-Oxley guide for finance and information technology professionals / Sanjay Anand.
12. Security Controls for Sarbanes-Oxley Section 404 IT Compliance: Authorization, Authentication, and Access / Dennis Brewer
13. The HIPAA Program Reference Book / Ross Leo
14. Manager's guide to compliance : Sarbanes-Oxley, COSO, ERM, COBIT, IFRS, BASEL II, OMB A-123, ASX 10, OECD principles, Turnbull guidance, best practices, and case studies / Anthony Tarantino
15. Rodney Ryder's Guide to BPO, Data Protection and Information Security / Rodney Ryder
16. Website : www.itgi.org

Suggested Evaluation Methods:

Assignments
Groups Presentations
Project Evaluation
Presentations

Parallel/Similar courses the existing curriculum:

S.No.	Name of the course	Institute where it was offered
	N.A.	

Name of Member					
Designation					
Org. / Inst.					
Signature					

Name of the Expert: Rohit Srivastava, Pawan Desai

Signature:

Date:3/8/2013