GUJARAT TECHNOLOGICAL UNIVERSITY

BRANCH: CYBER SECURITY (59)

SUBJECT NAME: RISK ASSESSMENT AND SECURITY AUDIT

SUBJECT CODE: 2725905

SEMESTER: II

Type of course: Master of Engineering(Cyber Security)

Prerequisite: Cyber security fundamentals

Rationale: Cyber security risk management guides a growing number of IT decisions. Cyber securities risks continue to have critical impacts on overall IT risk modeling, assessment and mitigation. The goal of this course is to teach students the risk management framework with both qualitative and quantitative assessment methods that concentrate on the information security (IS) aspect of IT risks. The relationship between the IT risk and business value will be discussed through several industry case studies.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks						Total Marks
				Theory Marks		Practical Marks				
L	T	P	C	ESE (E)	PA (M)	ESE (V)		PA (I)		
						ESE	OEP	PA	RP	
4	0	2	5	70	30	20	10	10	10	150

Content:

Sr. No.	Content	Total Hours	%Weightage
1.	Introduction, what is risk and risk management, risk assessment, monitoring and review, cyberspace, cyber system.	2	5%
2.	What is cyber security, how does cyber security relate to information security, how does cyber security relate to critical infrastructure protection, how does cyber security relate to safety, What is cyber risk, communication and consultation of cyber risk, cyber risk assessment, monitoring and review of cyber risk	4	10%
3.	Context establishment, context, goals and objectives, target of assessment, interface to cyberspace and attack surface, scope, focus and assumption, assets, scale and risk evaluation criteria,	2	5%
4.	Risk identification techniques, malicious risks, non-malicious risks, risk analysis, threat analysis, vulnerability analysis, likelihood of incidents, consequences of incidents	4	10%
5.	Risk evaluation, consolidation of risk analysis results, evaluation of risk level, risk aggregation, risk grouping, risk treatment identification, risk acceptance	3	5%
6.	Two-factor measure, three-factor measure, many-factor measure, which measure to use for cyber risk?, classification of scales, qualitative versus quantitative risk assessment, scale for likelihood, scale for consequence, what scale to use for cyber risk	3	5%
7.	Defining information security metrics	5	10%
8.	Risk analysis techniques	5	10%

9.	Automating metric calculations and tools	5	10%
10.	What is an IT security assessment, what is an IT security audit, what is compliance, how does and audit differs from assessment, case study: Enron, WorldCom, TJX Credit Card Breach	2	5%
11.	Organization do to be in compliance, Auditing within IT infrastructure, managing IT compliance	3	5%
12.	Auditing standards and frameworks, COSO, COBIT, ISO/IEC 27001 standard, ISO/IEC 27002 standard, NIST 800-53	4	10%
13	Industry case studies	6	10%

Reference Books:

1. Cyber-Risk Management by AtleRefsdal, Bj¢rnarSolhaug and KetilSt¢len - Springer

2. Auditing IT Infrastructures for Compliance by Marty M. Weiss and Michael G. Solomon – Jones & Bartlett Learning

3. Quantitative Risk Assessment: The Scientific Platform by TerjeAven – Cambridge University Press

4. Information Security Risk Assessment Toolkit by Mark Talabis and Jason Martin – Elseview

5. IT Security Risk Control Management – An Audit Preparation Plan by Raymond Pompon – Apress

Course Outcome:

After learning this course, the students should able to:

1. Design information security risk management framework and methodologies
2. Identify and modeling information security risks
3. Judge the difference between qualitative and quantitative risk assessment methods
4. Articulate information security risks as business consequences

List of Experiments:

1. To audit the c/c++ or Python code using RATS code checking tool.
2. Implement Flawfinder stand-alone script to check for calls to know potentially vulnerable library function calls.
3. Implement FindBugs standalone GUI application,or Eclipse plugin for loading custom rules set.
4. Implement pychecker stand-alone script to find bugs in the code.

5. Installation of splunk and study basic working as to stores data in its index and therefore separate database required

6. Implement splunk to discovers useful information automatically without searching manually

7. Implement splunk to converts log data into Visual graphs and reports to simplify analysis, reporting and troubleshooting

8. Submit a report on cyber security risk assessment for SCADA and DCS networks.