Integral University Lucknow
Study & Evaluation Scheme
B. Tech. (CSE) Cloud Technology and Information Security

SEMESTER 5

Sl. No	Subject Code	Category	Subject	Periods				Evaluation Scheme				Subject Total
								Sessional			Exam	
				L	T	P	C	CT	TA	CA	ESE	
1	CS-361	HM	Logical Reasoning and Thinking	2	1	0	3	25	15	40	60	100
2	CS-353	DC	Storage Technologies	2	1	0	3	25	15	40	60	100
3		DE	Departmental Elective I	3	1	0	4	25	15	40	60	100
4	CS-357	DC	Installation & Configuration of Server	3	1	0	4	25	15	40	60	100
5	CS-355	DC	Ethical Hacking	3	1	0	4	25	15	40	60	100
6	CS-351	DC	Cloud Technology	3	1	0	4	25	15	40	60	100
7	CS-354	DC	Storage Technologies Lab	0	0	2	1	30	30	60	40	100
8	CS-356	DC	Ethical Hacking Lab	0	0	2	1	30	30	60	40	100
9	CS-358	DC	Installation & Configuration of Server Lab	0	0	2	1	30	30	60	40	100
10	CS-352	DC	Cloud Technology Lab	0	0	2	1	30	30	60	40	100
			TOTAL	**16**	**6**	**8**	**26**	**270**	**210**	**480**	**520**	**1000**

SEMESTER 6

Sl. No	Subject Code	Category	Subject	Periods				Evaluation Scheme				Subject Total
								Sessional			Exam	
				L	T	P	C	CT	TA	CA	ESE	
1		OE	Open Elective-1	-	-	-	4	25	15	40	60	100
2	CS 371	DC	Web Technology	3	1	0	4	25	15	40	60	100
3	CS 372	DC	Theory of Automata and Compiler Design	3	1	0	4	25	15	40	60	100
4	CS 373	DC	Cloud Security	2	1	0	3	25	15	40	60	100
5	CS 374	DC	Principles of Virtualization	3	1	0	4	25	15	40	60	100
6	CS 375	DC	Infrastructure Solutions on Cloud	2	1	0	3	25	15	40	60	100
7		DE	Departmental Elective II	3	1	0	4	25	15	40	60	100
8	CS 376	DC	Infrastructure Solutions on Cloud Lab	0	0	2	1	30	30	60	40	100
9	CS 377	DC	Principles of Virtualization Lab	0	0	2	1	30	30	60	40	100
10	CS 399	P	Mini Project-I	0	0	2	1			60	40	100
			TOTAL	**16**	**6**	**6**	**29**	**235**	**165**	**460**	**540**	**1000**

SEMESTER 7

Sl. No	Subject Code	Category	Subject	Periods				Evaluation Scheme				Subject Total
								Sessional			Exam	
				L	T	P	C	CT	TA	CA	ESE	
1		DE	Departmental Elective III	3	1	0	4	25	15	40	60	100
2	CS 461	DC	Cyber Forensics & Investigation	3	1	0	4	25	15	40	60	100
3	CS 462	DC	Cloud Web Services	3	1	0	4	25	15	40	60	100
4	CS 463	DC	Linux Administration	2	1	0	3	25	15	40	60	100
5	CS 464	DC	Disaster Recovery and Business Continuity Management	2	1	0	3	25	15	40	60	100
6		DE	Departmental Elective IV	3	1	0	4	25	15	40	60	100
7	CS 465	DC	Cyber Forensics & Investigation- Lab	0	0	2	1	30	30	60	40	100
8	CS 466	DC	Cloud Web Services Lab	0	0	2	1	30	30	60	40	100
9	CS 467	DC	Linux Administration Lab	0	0	2	1	30	30	60	40	100
10	CS 479	P	Mini Project – 2	0	0	2	1	-	-	60	40	100
11	CS300	P	Industrial Training*	-	-	-	0	0	0	100	0	100
			TOTAL	13	5	8	26	240	180	480	520	1000

*A student must clear this paper with 50% passing marks up to the final year and marks will not be included in result.

SEMESTER 8

Sl. No	Subject Code	Category	Subject	Periods				Evaluation Scheme				Subject Total
								Sessional			Exam	
				L	T	P	C	CT	TA	CA	ESE	
1	CS 481	DC	IT Infrastructure Library	2	1	0	3	25	15	40	60	100
2		OE	Open Elective-II	-	-	-	4	25	15	40	60	100
3	CS 499	DC	B.Tech Project	-	-	8	4	-	60	60	40	100
4	CS 499	DC	B.Tech Project	-	-	8	4	-	60	60	40	100
5	CS 499	DC	B.Tech Project	-	-	8	4	-	60	60	40	100
6	CS 452	DC	Comprehensive Viva	-	-	-	0	-	100	100		100
			TOTAL	**2**	**2**	**24**	**19**	**50**	**310**	**360**	**240**	**600**

L – Lecture **T** – Tutorial **P** – Practical **C** – Credits **CT** – Class Test **TA** – Teacher Assessment

Sessional Total (CA) = Class Test + Teacher Assessment

Subject Total = Sessional Total (CA) + End Semester Examination (ESE)

BS – Basic Sciences **DC –** Departmental Core

HM – Humanities **OE** – Open Elective
DE – Departmental Elective **ESA** – Engineering Sciences & Arts (Foundation Course & Engineering Courses)

4

Departmental Elective I

- Security Architecture   CS-359
- Database Security CS 363
- Server Security   CS 364
- Any Online MOOC from the suggested list by the Department. Duration should be of at least 12 weeks so as to fulfil 4 credits

Departmental Elective II

- Information Security Emerging Trends   CS 378
- Cyber Security Incident Response Management   CS 379
- Application Security   CS 380
- Any Online MOOC from the suggested list by the Department. Duration should be of at least 12 weeks so as to fulfil 4 credits

Departmental Elective III

- Exchange Server Administration   CS 468
- Advanced Virtualization   CS 469
- Infrastructure Automation   CS 470
- Any Online MOOC from the suggested list by the Department. Duration should be of at least 12 weeks so as to fulfil 4 credits

Departmental Elective IV

- IT Governance, Risk and Information Security Management   CS 471
- COBIT VALIT RISKIT   CS 472
- ISO 27001, PCI DSS & HIPAA   CS 473
- Any Online MOOC from the suggested list by the Department. Duration should be of at least 12 weeks so as to fulfil 4 credits

Logical Reasoning and Thinking

L	T	P	C
2	1	0	3

Recommended Prerequisite –None   **Co-requisite** - None

Unit I: Verbal ability
Synonyms**,** AntonymsandOne word substitutes [3]

Unit II: Basic quantitative aptitude
Speed, Time and Distance, Time and Work, Linear Equations, Progressions (Sequences & Series), Permutation and Combination, Probability, Functions, Set Theory, Number Systems, LCM and HCF, Percentages, Collection and Scrutiny of data: Primary data, questionnaire and schedule; secondary data, their major sources including some government publications.   [8]

Unit III: Logical Reasoning - I
Number and Letter Series, Calendars, Clocks, Cubes, Venn Diagrams, Binary Logic, Seating Arrangement, Logical Sequence, Logical Matching, Logical Connectives, Syllogism.Blood Relations; concept of a statistical population and sample from a population; qualitative and quantitative data.[6]

Unit IV: Measures of Central Tendency
Objective of averaging, characteristics of good average, types of average, arithmetic mean of grouped and ungrouped data, correcting incorrect values, weighted arithmetic mean
Median - median of grouped and ungrouped data merit and limitation of median, computation of quartile, decile and percentileMode - calculation of mode of grouped and ungrouped data, merits and limitation of mode, relationship between mean, median and mode. Geometric mean and Harmonic mean.[10]

Unit V: Presentation of Data
Construction of tables with one or more factors of classification; Diagrammatic and Graphical representation of non-frequency data; Frequency distribution, cumulative frequency distribution and their graphical representation - histogram, Column Graphs, Bar Graphs, Line Charts, Pie Chart, Data Interpretation – Introduction and approaches [8]

Reference Books:
1. Richard I Levin, David S. Rubin: Statistics for Management, Pearson Prentice Hall Education Inc. Ltd, NewDelhi, 5th Ed. 2007

2. Bajpai, N. Business Statistics, Pearson, 2010
3. Sharma J.K., Business Statistics, Pearson Education India, 2010.
4. Anderson; David R, Dennis J. Sweeney and Thomas A. Williams, Quantitative Methods for Business, Prentice-Hall, WestPublishing Company, 1996.
5. CAT Complete course, UPKAR publications

Storage Technologies

L	T	P	C
2	1	0	3

Recommended Prerequisite – None   **Co-requisite** - None

Unit I: Introduction to Information storage and Management
Information Storage: Data – Types of Data –Information - Storage , Evolution of Storage Technology and Architecture, Data Center Infrastructure - Core elements- Key Requirements for Data Center Elements -Managing Storage Infrastructure, Key Challenges in Managing Information, Information Lifecycle - Information Lifecycle Management - ILM Implementation -ILM Benefits. [6]

Unit II: Storage System Environment
Components of a Storage System Environment – Host –Connectivity – Storage, Disk Drive Components –Platter – Spindle - Read/Write Head - Actuator Arm Assembly - Controller - Physical Disk Structure - Zoned Bit Recording - Logical Block Addressing , Disk Drive Performance -1 Disk Service Time , Fundamental Laws Governing Disk Performance , Logical Components of the Host - Operating System - Device Driver -Volume Manager - File System – Application , Application Requirements and Disk Performance. [8]

Unit III: RAID and Storage Networking Technologies
Implementation of RAID - Software RAID - Hardware RAID -RAID Array Component -RAID Levels - Striping -Mirroring -Parity RAID 0 RAID 1 -Nested RAID -RAID 3 -RAID 4 -RAID 5 --RAID 6 -RAID Comparison -RAID Impact on Disk-Performance - Application IOPS and RAID Configurations - Introduction to Direct Attached Storage – Types of DAS – Introduction to SAN – Components of SAN – FC connectivity – FC topologies – Introduction to NAS – NAS components – NAS Implementation – NAS File sharing [8]

Unit IV: Backup and Recovery
Introduction to Business Continuity - Backup Purpose -Disaster Recovery - Operational Backup –Archival, Backup Considerations, Backup Granularity, Recovery Considerations, Backup Methods , Backup Process, Backup and Restore Operations, Backup Topologies - Server less Backup , Backup Technologies -Backup to Tape - Physical Tape Library - Backup to Disk - Virtual Tape Library [7]

7

Unit V: Replication – Local and Remote
Source and Target -Uses of Local Replicas, Data Consistency - Consistency of a Replicated File System - Consistency of a Replicated Database , Local Replication Technologies - Host-Based Local Replication - Storage Array-Based Replication , Res tore and Restart Considerations - Tracking Changes to Source and Target , Creating Multiple Replicas, Management Interface – Remote Replication Modes – Remote Replication Technologies – Network Infrastructure [6]

Reference Books:
1. EMC Education Services, "Information Storage and Management: Storing, Managing, and Protecting Digital Information", Wiley Publishing Inc., 1st edition, 2009Bajpai, N. Business Statistics, Pearson, 2010.
2. Robert Spalding , "Storage Networks: The Complete Reference ", Tata McGraw Hill Publication, 2003

Security Architecture

L	T	P	C
3	1	0	4

Recommended Prerequisite –None   **Co-requisite** - None

Unit I: Introduction to Security Architecture
Origins of Architecture, managing complexity, information systems architecture, security architecture, benefits of architectural approach to information security, need for a holistic approach, security architecture model – SABSA, matrix, case studies [6]

Unit II: Phased Approach to build Security Architecture
Security Architecture – business drivers and traceability, using SABSA model to define a development process, strategy and concept phase, design phase, implementation phase, manage and measure phase, overview of enterprise security architecture, case studies [8]

Unit III: Contextual and Conceptual Security Architecture
Business context, aligning business objectives with security architecture, operational risk and impact assessment, influence of business processes, workflow, organizational structure on security architecture, location and time dependencies, security architectural layering, entity model and trust framework, security domain model, case studies[9]

8

Unit VI: Security Architecture Design
Logical-information flow, policies and services, application and system environment, security management and lifecycle, Physical-rules, mechanisms, policies, standards and procedure, user, platform and network infrastructure, Component-products and tools, Operations, case studies[9]

Unit V: Management of Security Architecture
Need for Security Management, best practices and maturity models, policy enforcement and compliance, components of security architecture management, product evaluation, managing service providers and third party security risks, balancing needs, requirements, risks and costs, impact of cloud, IoT and AI technologies on security architecture, case studies[8]

Reference Books:
1. Enterprise Architecture and Information Assurance: Developing a Secure Foundation by James A. Scholz, Auerbach Publications; 1 edition, 2013
2. Designing Security Architecture Solutions 1st Kindle Edition by Jay Ramachandran
3. Network Security Architectures (Networking Technology) 2nd Kindle Edition by Sean Convery
4. Threat Modeling: Designing for Security (MISL-WILEY) by Adam Shostack, Wiley, 2014
5. Enterprise Security Architecture: A Business-Driven Approach 1st Kindle Edition by Nicholas A Sherwood

Database Security

L	T	P	C
3	1	0	4

Recommended Prerequisite – None   **Co-requisite** - None

Unit I: Concepts of Database Security Management System

Database security concept, Importance of data, Levels of data security, Authorization in databases, Issues in database security, Concept of Least Privilege in User ID for databases. Perimeter security, firewalls, intrusion detection, and intrusion prevention. [6]

Unit II: Concepts of NoSQL

No SQL databases introduction, Differences from classical DBMS concepts with NoSQL, Advantages of NoSQL like Elastic Scaling, Big Data, Goodbye DBAs', Economics/Cost, Flexible Data models. Non/ partial applicability of ACID (Atomicity, Consistency, Isolation, Durability), BASE Properties, CAP theorem, comparison to traditional RDBMS databases. Horizontal scalability, Benefits of NoSQL Databases compared to traditional Databases.

Concept of UnSQL or Unstructured Query Language, Concept of Key Value & Tuple Store Databases, Concept of Graph Databases, Concept of Multimodel Databases [10]

Unit III: Encryption and Permissions in SQL Server 2012

Facility and Supply Recovery strategies. User Recovery strategies. Technical Recovery strategies, Data Recovery strategies, Activation Phase- Major Disaster or Disruption, Intermediate Disaster or Disruption, Minor Disaster, Activating BC/DR Teams, Developing Triggers, Transition Trigger. Defining BC/DR Team and Key Personnel, Defining Tasks, Assigning Resources, Communication Plan. [8]

Unit VI: Security of SQL Server 2012

User authorization, authentication and security, protecting data using permissions, roles, schemas, SQL firewall, web application firewall, securing dynamic SQL from injections, protecting SQL server from DoS and injection attacks. [6]

Unit V: SQL Server Auditing

Auditing – Using the profiler to audit SQL server access, using DML trigger for auditing data modification, Using DDL triggers for auditing structure modification, configuring SQL server auditing, auditing and tracing user configurable events, policy based management, system centre advisor to analyze instances [10]

Text Books:

1. Information Systems Security: Security Management, Metrics, Frameworks and Best Practices by Nina Godbole, Wiley, 1st ed; 2008
2. Database security by SilvanaCastano, 2nd Edition, Pub: Addison-Wesley Professional, 2008
3. Microsoft SQL server 2012 Security Cookbook by Rudi Bruchez, Pub: PACKT publishing, 1st ed; 2012.

Reference Books:

1. Handbook of database security: Applications and Trends Michael Gertz, SushilJajodia, Pub: Springer, 1st ed; 2008
2. Implementing database security and auditing, Ron Ben-Natan, Pub: Digital Press, 1st ed; 2005

Server Security

L	T	P	C
3	1	0	4

Recommended Prerequisite – None   **Co-requisite** - None

Unit I: Conceptual understanding on Server Security

User authentication and authorization – limiting system access and controlling using behavior, restricting access to software, restricting software access to resources, controlling access to data, EFS basics, maintenance and recovery strategies, security risk assessment of servers – high, medium, low risk servers and applications and development of server security policy, important steps to improve security of servers, server security principles.[8]

Unit II: Techniques for Securing Server

Implementing physical security, Server hardening – OS and hardware, important ports, services and protocols that improve server security, key steps to be followed while planning and deployment, user administration, password management, encryption, configuring logging, vulnerability scanning and penetration testing.[6]

Unit III: Securing Windows and Linux Servers

Windows server 2012 R2 OS and baseline security configuration, SCM, Active Directory, AppLocker and PowerShell, server types and roles, SMB configuration and encryption, baseline application security, BitLocker, network services security, auditing and monitoring, overview of Red Hat Enterprise Linux 6 server security, using TCP Wrappers, enhancing security with xinetd, securing portmap, NIS, NFS, FTP, Postfix, Sendmail, securing Apache HTTP server[9]

Unit IV: Securing SQL Server

Understanding threats to SQL server using STRIDE and DREAD methods, SQL server security model – security principal hierarchy, instance level security, logins, server roles, credentials, database level security, users and roles, data-level security – schemas, RLS, dynamic data masking, encryption in SQL server, securing metadata, important security configurations for DBAs, understanding MySQL server security [6]

Unit V: Securing Web Server

11

Securing Apache 2.4 webserver OS, configuring access controls, securing web content, authentication and encryption techniques, key security configurations in web server, tools and techniques used for web server security, using checklist for web server security assessment, securing Apache, Nginx server as reverse-proxy [6]

Text Books:

1. NIST's Guide to General Server Security Special Publication 800-123
2. CompTIA Server+ Study Guide by Troy McMillan, Sybex; Study Guide edition (26 July 2016)
3. Getting Started with Windows Server Security by SanthoshSivarajan, Packt Publishing Limited (27 February 2015)
4. Linux Server Security: Hack and Defend by Chris Binnie, Wiley (2016)
5. Red Hat Enterprise Linux 6 Security Guide
6. Practical Linux Security Cookbook by Tajinder Singh Kalsi, Packt Publishing Limited (29 April 2016)

Reference Books:

1. Securing SQL Server: DBAs Defending the Database by Peter A. Carter, Apress; 1st ed. edition (19 November 2016)
2. NIST's Guidelines on Securing Public Web Servers SP 800-44 v2
3. A Web Developer's Guide to Securing a Server (Web Security Topics) by Nigel Chapman, Jenny Chapman, Macavon Media (22 November 2011)
4. Securing SQL Server: Protecting Your Database from Attackers by Denny Cherry, Syngress; 3 edition (24 April 2015)

Installation & Configuration of Server

L	T	P	C
3	1	0	4

Recommended Prerequisite –None   **Co-requisite** - None

Unit I: Creating and Configuring Virtual Network in Windows

What is Virtual Networking, how to create New Virtual Switch, configuration of MAC Addresses, how to create Virtual Network Adapters, Synthetic Adaptors and Emulated Adapters, Configuration of Hardware Acceleration Setting and Advanced Network Adapter Features, Configure Virtual Network, Extending a Production Network into Virtual Space, creating an Isolated Network. [6]

Unit II: Configuring IPv4 and IPv6 Addressing in Windows

IPv4 Classful Addressing, Subnetting, Classless Inter-Domain Routing with Example, Public and Private IPv4 Addressing, Using Network Address Translation and Proxy Server, IPv4 Subnetting and Supernetting, Assigning IPv4 Addressing and Configuration, Dynamic Host Configuration Protocol, Automatic Private IP Addressing(APIPA), Introducing IPv6, IPv6 Address types, Global Unicast Addresses, Link-Local Unicast Addresses, Unique Local Unicast Addresses, Special, Multicast, Anycast Addresses, Assigning IPv6 Addresses, Manual IPv6 Address Allocation, Stateless IPv6 Address Auto configuration, Dynamic Host Configuration Protocol [10]

Unit III: Deploying and Configuring the DHCP, DNS Service

Understanding DHCP, DHCP Packets, DHCP message types option, pad option, option overload option, Vendor-Specific information Option, DHCP Communications and Lease Negotiation, DHCP Lease Renewal, Designing a DHCP Infrastructure, a Distributed DHCP and Centralised DHCP Infrastructures, a Hybrid DHCP Infrastructure and DHCP Network Traffic,How to create DNS Standard, how to create DNS Domain Hierarchy, Understanding DNS Communications, Comprehending DNS Server Caching, Understanding DNS Referrals and Queries, function of DNA Forwarders and Reverse Name Resolution, Designing DNS Deployment, Resolving Internet Names, Hosting internet Domains, Hosting Active Directory Domain, Integrating DHCP and DNS, Separating DNS Services [8]

Unit IV: Installing Domain Controllers

Understanding Active Directory and Active Directory Architecture Functions, function of Objects and Attributes, Understanding Domains, Zooming in: Organizational Units, Zooming in: Groups, Zooming out: Domain Trees, Zooming out: Forests, Introducing LDAP, function of Replication, Installing the Active Directory Domain Services Role, Creating a New Forest, Adding a Domain Controller to an Existing Domain, Creating a New Child Domain in a

Forest, Installing AD DS on Server Core, install from media(IFM), Upgrading Active Directory Domain Services, Removing a Domain Controller, configuring the Global Catalog [8]

Unit V: Creating and Managing Active Directory Groups and Organizational Units
Designing an Internal Domain Structure, how Inheritance works, how organizational Units and Group objects, Working with Organizational Units, creating OUs, using OUs to Delegate Active Directory, Management Tasks, Working with Groups, function of Group types and group scopes, Domain Local Groups, Global Groups and universal Groups, Nesting groups, Creating groups from the command line, Managing Group Memberships, Managing Group Membership using Group Policy, Managing group objects with Dsmod.exe, converting Groups, Deleting a Group[8]

Reference Books:
1. Windows Server 2012: A Handbook for Professionals by Aditya Raj (Author)
2. MCSA 70-410 Cert Guide R2: Installing and Configuring Windows Server 2012 (Certification Guide) Hardcover – Import, 12 Sep 2014 by Don Poulton (Author), David Camardella (Author)
3. Installing and Configuring Widows Server 2012 by Craig Zacker
4. Mastering Windows Server 2012 R2 by Mark Minasi, Kevin Greene, Christian Booth, Robert Butler

Ethical Hacking

L	T	P	C
3	1	0	4

Recommended Prerequisite – None   **Co-requisite** - None

Unit I: Introduction to Ethical Hacking
Hacking Methodology, Process of Malicious Hacking, and Foot printing and scanning: Foot printing, scanning. Enumeration: Enumeration. System Hacking and Trojans: System Hacking, Trojans and Black Box Vs. White Box Techniques. [8]

Unit II: Hacking Methodology
Denial of Service, Sniffers, Session Hijacking and Hacking Web Servers: Session Hijacking, Hacking Web Servers. Web Application Vulnerabilities and Web Techniques Based Password Cracking: Web Application Vulnerabilities, Web Based Password Cracking Techniques.[8]

Unit III: Web and Network Hacking
SQL Injection, Hacking Wireless Networking, Viruses, Worms and Physical Security: Viruses and Worms, Physical Security. Linux Hacking: Linux Hacking. Evading IDS and Firewalls: Evading IDS and Firewalls.

[8]

Unit VI: Report writing & Mitigation
Introduction to Report Writing & Mitigation, requirements for   low level reporting & high level reporting of Penetration testing results, Demonstration of vulnerabilities and Mitigation of issues identified including tracking. [8]

Unit V: Ethical Hacking and Legal System:
Overview of India's Information Technology Amendment Act 2008 (IT Act 2008), hacker vs cracker, liabilities – civil and penal, cyber theft and IPC sec 378, IT Act 2008 – sections 43, 65 and 66, how to file a complaint of suspected hacking, Case Studies, understanding how hacking is legally dealt with among BRICS countries [8]

Reference Books:
1. Gray Hat Hacking The Ethical Hackers Handbook, 3rd Edition Paperback – 1 Jul 2017 by Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, McGraw Hill Education; 3 ed (1 July 2017)

2. CEH v9: Certified Ethical Hacker Version 9 Study Guide by Sean-Philip Oriyano, Sybex; Stg edition (17 June 2016)

3. Hacking for Beginners: Ultimate 7 Hour Hacking Course for Beginners. Learn Wireless Hacking, Basic Security, Penetration Testing by Anthony Reynolds, CreateSpace Independent Publishing Platform (10 April 2017)

4. An Ethical Guide To WI-FI Hacking and Security by SwaroopYermalkar, BecomeShakespeare.com; First edition (15 August 2014)

5. Hands-On Ethical Hacking and Network Defense by Michael T. Simpson | Kent Backman | James Corley, Cengage India 1st edition (2016)

6. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy by Patrick Engebretson, Syngress; 2 edition (12 September 2013)

7. Hacking With Python: The Complete Guide to Ethical Hacking, Basic Security, Botnet Attack, Python hacking and Penetration Testing Kindle Edition by John C. Smalls

Cloud Technology

L	T	P	C
3	1	0	4

Recommended Prerequisite –None   **Co-requisite** - None

Unit I: Introduction
Introduction to Cloud Computing, History and Evolution of Cloud Computing, Types of clouds, Private Public and hybrid clouds, Cloud Computing architecture, Cloud computing infrastructure, Merits of Cloud computing, , Cloud computing delivery models and services (IaaS, PaaS, SaaS), obstacles for cloud technology, Cloud vulnerabilities, Cloud challenges, Practical applications of cloud computing.[6]

Unit II: Cloud Computing Companies and Migrating to Cloud
Web-based business services, Delivering Business Processes from the Cloud: Business process examples, Broad Approaches to Migrating into the Cloud, The Seven-Step Model of Migration into a Cloud, Efficient Steps for migrating to cloud., Risks: Measuring and assessment of risks, Company concerns Risk Mitigation methodology for Cloud computing, Case Studies.[8]

Unit III: Cloud Cost Management and Selection of Cloud Provider
Assessing the Cloud: software Evaluation, System Testing, Seasonal or peak loading, Cost cutting and cost-benefit analysis, selecting the right scalable application. Considerations for selecting cloud solution. Understanding Best Practices used in selection of Cloud service and providers, Clouding the Standards and Best Practices Issue: Interoperability, Portability, Integration, Security, Standards Organizations and Groups associated with Cloud Computing, Commercial and Business Consideration [10]

Unit IV: Governance in the Cloud
Industry Standards Organizations and Groups associated with Cloud Computing, Need for IT governance in cloud computing, Cloud Governance Solution: Access Controls, Financial Controls, Key Management and Encryption, Logging and Auditing, API integration. Legal Issues: Data Privacy and Security Issues, Cloud Contracting models, Jurisdictional Issues Raised by Virtualization and Data Location, Legal issues in Commercial and Business Considerations [8]

Unit V: Ten Cloud DO and DONTS:
Don't be reactive, do consider the cloud a financial issue, don't go alone, do think about your architecture, don't neglect governance, don't forget about business purpose, do make security the centerpiece of your strategy, don't apply the cloud to everything, don't forget about Service Management, do start with a pilot project. [8]

Reference Books:

16

1. RajkumarBuyya, James Broberg, Andrzej M. Goscinski, "Cloud Computing: Principles and Paradigms", John Wiley and Sons Publications, 2011
2. Christopher Barnett, "Brief Guide to Cloud Computing", Constable & Robinson Limited, 2010
3. BorivojeFurht, Armando Escalante, "Handbook on Cloud Computing" , Springer, 2010

Storage Technologies Lab

L	T	P	C
0	0	2	1

Recommended Prerequisite –Storage TechnologiesCo-requisite– None

List of Programs:

1. Creating raw partitions and make a file system in server
2. Create volumes , extend and shrink the volumes
3. Configure RAID 1 (mirroring) that replicates the data in two different disks
4. Configure RAID 5 that shows the data striping with parity
5. Configure storage area network in server 2012
6. Configure iSCSI in server 2012
7. Configure and deploy NAS in server 2012
8. Create and use the virtual hard disk in Windows 7
9. Configuring the virtual disk to an existing virtual machine(VM)
10. Attaching different virtual disk formats in an existing VM with no downtime

Ethical Hacking Lab

L	T	P	C
0	0	2	1

Recommended Prerequisite –Ethical Hacking**Co-requisite** - None

List of Programs:

1. Passive Reconnaissance using "Who is" and Online tools
2. Active Reconnaissance using "Sampad" and web site details
3. Full Scan, Half Open Scan and Stealth scan using "nmap"
4. UDP and Ping Scanning using "Advance Lan Scanner" and "Superscan"
5. Packet crafting using "Packet creator" tools
6. Exploiting NetBIOS vulnerability
7. Password Revelation from browsers and social networking application
8. Creating and Analyzing spoofed emails
9. Creating and Analyzing Trojans
10. OS password cracking

Installation & Configuration of Server Lab

L	T	P	C
0	0	2	1

Recommended Prerequisite –Installation & Configuration of ServerCo-requisite - None

List of Programs:

1. Installation windows Server 2012.
2. Configuration for Windows Server.
3. Configuration Local Storage for Windows Server.
4. Configuration File and Share Access for Windows Server.
5. Configuration Print and Document Services for Windows Server.
6. Configuration windows server for Remote Management.
7. Creating Virtual Machine in Windows Server.
8. Configuration and Setting Virtual Machine.

Cloud Technology Lab

L	T	P	C
0	0	2	1

Recommended Prerequisite –Cloud TechnologyCo-requisite - None

List of Programs:

1. Study the basic cloud architecture and represent it using a case study
2. Enlist Major difference between SAAS PAAS & IAAS also submit a research done on various companies in cloud business and the corresponding services provided by them , tag them under SAAS PAAS & IAAS.
3. Study and present a report on Jolly cloud.
4. Present a report on obstacles and vulnerabilities in cloud computing on generic level
5. Present a report on Amazon cloud services.
6. Present a report on Microsoft cloud services.
7. Present a report on cost management on cloud
8. Enlist and explain legal issues involved in the cloud with the lelp of a case study
9. Explain the process of migrating to cloud with a case study.
10. Present a report on google cloud and cloud services.

Web Technology

L	T	P	C
3	1	0	4

Recommended Prerequisite – None   **Co-requisite** - None

Unit I: Introduction to the Internetand the World Wide Web

Introduction, History of internet, Internet Design Principles, Internet Protocols - FTP, TCP/IP, SMTP, Telnet, etc., Client Server Communication, Web System architecture.Evolution of the Web, Web architectures, Web clients and servers, Static and Dynamic Web Applications, Front end and back end web development. HTML, CSS, JS, XML; HTTP, secure HTTP, etc; URL, Web Services – SOAP, REST.[8]
.

Unit II: HTML & CSS

Introduction to Html, Html Document structure, Html Editors, Html element/tag & attributes, Designing simple page - Html tag, Head tag, Body tag; More Html tags - Anchor tag, Image tag, Table tag, List tag, Frame tag, Div tag ; Html forms - Input type, Text area, Select , Button, Images. Introduction to CSS, Syntax, Selectors ,Embedding CSS to Html, Formatting fonts, Text & background colour, Inline styles, External and Internal Style Sheets, Borders & boxing.[10]

Unit III: XML and HTML5, CSS3

Introduction to XML, Difference b/w Html & XML, XML editors, XML Elements & Attributes XML DTD, XML Schema, XML Parser, Document Object Model (DOM), XML DOM.Introduction to HTML5,CSS3, New features, Local storage, Web Sockets, Server events, Canvas, Audio & Video, Geolocation, Microdata, Drag and Drop. Browser life cycle and browser rendering stages. Service workers.[8]

Unit IV: PHP Server side scripting

Introduction to PHP, Basic Syntax, Variables, constants and operators, Loops, Arrays and Strings, Environment & environment variables, responding to HTTP requests, Files, Cookies, Sessions, Examples.[7]

Unit V: Practical website development

Commonly used Web Servers and browsers, Setting up a server and domain name, website types and structures, web authoring tools, Web hosting, website maintenance, generating traffic to your website.[7]

21

.
Reference Books:
1. Introducing Web Development, Jorg Krause. Apress 2017.
2. HTML & CSS: The Complete Reference, Thomas Powell. McGraw Hill, Fifth Edition, 2010
3. Creating a Website: The Missing Manual, 3rd Edition, Mathew Macdonald. O'Reilly
4. Web Technologies - HTML, JavaScript, PHP, Java, JSP, ASP.NET, XML and Ajax Black, Kogen Learning Systems (Dreamtech Press), 5th Edition 2009.
5. HTML, XHTML & CSS Bible, Brian Pfaffenberger, Steven M.Schafer, Charles White, Bill Karow- Wiley Publishing Inc, 2010
6. HTML5 & CSS3 for the Real World, 2 Edition, Alexis Goldstein, Estelle Weyl, Louis Lazaris. Apress 2015.
7. HTML5 & CSS3 for Dummies, Andy Harris. Wiley 2014.
8. Learning PHP A Gentle Introduction to the Web's Most Popular Language, David Sklar. O'Reilly 2016.
9. Build Your Own Database Driven Web Site Using PHP & MySQL, Kevin Yank. Sitepoint , 4th Edition, 2009.

Theory of Automata and Complier Design

L	T	P	C
3	1	0	4

Recommended Prerequisite –None   **Co-requisite** - None

UNIT I:
Introduction to Compiler, Phases and passes, Bootstrapping.
Formal Language and Regular Expressions: Languages, Definition Languages regular expressions, Finite Automata DFA, NFA. Conversion of regular expression to NFA, NFA to DFA. Applications of Finite Automata to lexical analysis, lex tools.
Context Free grammars and parsing: Context free grammars, derivation, parse trees, ambiguity LL(K) grammars and LL(1) parsing[8]

UNIT II:
S R Parsers: Bottom up parsing handle pruning LR Grammar Parsing, LALR parsing, parsing ambiguous grammars, YACC programming specification.

22

Semantics: Syntax directed translation, S-attributed and L-attributed grammars, Intermediate code – abstract syntax tree, translation of simple statements and control flow statements.

Context Sensitive features – Chomsky hierarchy of languages and recognizers. Type checking, type conversions, equivalence of type expressions, overloading of functions and operations.[8]

UNIT III:
Push Down Automata (PDA): Description and definition, Instantaneous Description, Language of PDA, Acceptance by Final state, Acceptance by empty stack, Deterministic PDA, Equivalence of PDA and CFG, CFG to PDA and PDA to CFG, Two stack PDA[7]

UNIT IV:
Turing machines (TM): Basic model, definition and representation, Instantaneous Description, Language acceptance by TM, Variants of Turing Machine, TM as Computer of Integer functions, Universal TM, Church's Thesis, Recursive and recursively enumerable languages, Halting problem, Introduction to Undecidability, Undecidable problems about TMs. Post correspondence problem (PCP), Modified PCP, Introduction to recursive function theory.[9]

UNIT V:
Code generation: Machine dependent code generation, object code forms.

Code optimization: Machine-Independent Optimizations, Loop optimization, DAG representation of basic blocks, value numbers and algebraic laws, Global Data-Flow analysis. [8]

Textbooks: 1. Aho, Sethi& Ullman, "Compilers: Principles, Techniques and Tools", Pearson Education
 2. V Raghvan, " Principles of Compiler Design", TMH Hopcroft and Ullman, "Introduction to Automata Theory Languages and Computation",Addison Wesley.
3. Mishra & Chandrasekhar, "Theory of Computer Sciences", PHI.
4. Martin, "Introduction to Languages & Theory of Computation", TMH.

Cloud Security

L	T	P	C
2	1	0	3

Recommended Prerequisite – None   **Co-requisite** - None

Unit I: Introduction to Virtualization Security
Introduction to Virtualization, impact and business benefits of Virtualization in the context of Security, Risks of Virtualization including attacks on Virtualization infrastructure, Hyper jacking and Virtual Machine jumping. Hyper jacking attacks like Blue Pill, Sub Virt, Vitriol, attacks on Virtualization features and compliance and Management challenges. Strategies and counter measures for addressing Virtualization risks, securing hypervisors, virtual machines threats, vulnerabilities and mitigation measures.[8]
.

Unit II: Introduction to Cloud Security
Introduction to Cloud Computing, various Cloud Delivery models including Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) in the context of Security, Cloud deployment models – public, private and hybrid in the context of Security, Trusted Cloud Initiative (TCI) and Cloud Trust Protocol (CTP), Transparency as a Service (TaaS) and Security as a Service (SecaaS), Cloud Security, Incident and Response (Cloud SIRT), Cloud Data Governance and Governance, Risk and Compliance (GRC) Stack, top threats to Cloud Security, comparison of traditional IT and Cloud Security.[9]

Unit III: Cloud Security Architecture
Architectural considerations, Cloud storage and data security, identity management and access control, autonomic security, encryption and key strategies, secure connection, Privacy in Cloud, architecture changes for different Cloud deployment models, Business Continuity Management and Disaster Recovery in the Cloud, OpenStack Cloud Security, Cloud forensics.[7]

Unit IV: Cloud Security Controls
Introduction to Cloud Controls Matrix, 13 domains of Security controls, fundamental security principles, deterrent, preventive, detective and corrective security controls for Cloud computing, assessing security risk of a cloud provider.[5]

Unit V: Security of Cloud Services

Cloud Platform and Infrastructure security-physical environment, networking, computing, virtualization, storage, risks and countermeasures, Cloud application security, Cloud secure development lifecycle, Cloud application architecture, multi-factor authentication, SSO, Understanding legal challenges involved in Cloud, liability, copyright, data protection, IPR, data portability, inter-country legal frameworks, personal data protection and privacy, data controller and processor, contracts, provider's insolvency risk.[6]
.

Reference Books:
1. Virtualization Security: Protecting Virtualized Environments by Dave Shackleford, Sybex (4 December 2012)
2. OpenStack Cloud Security by Fabio Alessandro Locati, Packt Publishing Limited (28 July 2015)
3. Cloud Security – A comprehensive Guide to Secure Cloud Computing by Ronald L. Krutz and Russel Dean Vines, Wiley, 2010
4. Cloud Security and Privacy by Mather Tim, Shroff Publishers & Distributers Private Limited - Mumbai; First edition (2009)
5. Securing the Cloud: Cloud Computer Security Techniques and Tactics by Vic (J.R.) Winkler, Syngress (1 June 2011)
6. Practical Cloud Security: A Cross-Industry View by Melvin B. Greer Jr., Kevin L. Jackson CRC Press; 1 edition (2 August 2016)
7. www.cloudsecurityalliance.org

Principles of Virtualization

L	T	P	C
3	1	0	4

Recommended Prerequisite – None   **Co-requisite** - None

Unit I: Basics of Virtualization
Understanding Virtualization, Need of Virtualization and Virtualization Technologies: Server Virtualization, Storage Virtualization, I/O Virtualization, Network Virtualization, Client Virtualization, Application virtualization, Desktop virtualization, Understanding Virtualization Uses: Studying Server Consolidation, Development and Test Environments , Helping with Disaster Recovery.[7]

Unit II: Deploying and Managing an Enterprise Desktop Virtualization Environment
Configure the BIOS to support hardware virtualization; Install and configure Windows Virtual PC: installing Windows Virtual PC on various platforms (32-bit, 64-bit), creating and managing virtual hard disks, configuring virtual machine resources including network resources, preparing host machines; create, deploy, and maintain images.[7]

Unit III: Deploying and Managing Presentation Virtualization Environment
Prepare and manage remote applications: configuring application sharing, package applications for deployment by using RemoteApp, installing and configuring the RD Session Host Role Service on the server.[8]

Unit IV: Accessing Published Applications
Access published applications: configuring Remote Desktop Web Access, configuring role-based application provisioning, and configuring Remote Desktop client connections. Configure client settings to access virtualized desktops: configuring client settings.[8]

Unit V: Understanding Virtualization Software
List of virtualization Software available .Vmware- introduction to Vsphere, ESXi, VCenterServer andVsphere client. Creating Virtual Machine.. Introduction to HYPER-V role. Create Virtual Machines. Create Hyper-v virtual networking, Use virtual Machine Snapshots. Monitor the performance of a Hyper-v server, Citrix XEN Desktop fundamentals.[10]

.
Reference Books:
1. Virtualization with Microsoft Virtual Server 2005 by TwanGrotenhuis, RogierDittner, Aaron Tiensivu, Ken Majors, Geoffrey Green, David Rule, Andy Jones, Matthijs ten Seldam, Syngress Publications, 2006
2. Virtualization--the complete cornerstone guide to virtualization best practices, Ivanka Menken, Gerard Blokdijk, Lightning Source Incorporated, 2008
3. Virtualization: From the Desktop to the Enterprise, Chris Wolf, Erick M. Halter, EBook, 2005

Infrastructure Solutions on Cloud

L	T	P	C
2	1	0	3

Recommended Prerequisite – None   **Co-requisite** - None

Unit I: Getting Started with Azure
Overview of Cloud Computing – Various Cloud Offerings – Azure Basics – Azure Services – Azure Portals – Preview Portal, Management Portal, Subscription Management – Billing – Pricing Calculator - **Azure Virtual Machines :**Virtual Machine(VM) Basics – Status, IP Address, Creating and Configuring Virtual Machines – Configuring VM disks – Virtual Machine Management[8]

Unit II: Azure Storage
Storage Basics – Storage Types – Azure Storage Offerings – Understanding Azure Regions – Using Storage Accounts – Enabling Larger and Faster Storage – Resizing Azure Disks – Using Premium Storage – Monitoring Azure Storage Accounts – Best Practices for Azure Storage – Azure VM Storage Types – Azure Files – Managing Azure Storage.[8]

Unit III: Azure Networking

Basics of Virtual Networks – Address Spaces, Subnets, DNS Servers – Creating and Using Virtual Networks – Network Security Groups – Virtual Appliances – Load Balancer basics – Configuring Load Balancers – Creating and Using Load balancers – Azure VPN[8]

Unit IV: Azure Active Directory

Introduction to Active Directory(AD), Identity and Authentication in Public Cloud – Introduction to Azure AD – Extending Active Directory into Azure – Azure AD and applications – Reporting and Monitoring Azure AD.[5]

Unit V: Azure Databases

SQL Azure: Creating a SQL Server - Creating a SQL DB - Creating Tables - Adding Data to the Table - View Connection Strings - Security Configurations - Migrating on premise DB to SQL Azure.

Azure Websites: Creating a Website, Setting deployment credentials -Choosing a platform -Setting up Default page for website - Scaling - Auto Scaling by Time -Auto Scaling by Metric - Difference between Free, Shared, Basic and Standard websites - Creating a website using Visual studio[6]

.
Reference Books:
1. **Michael Collier, Robin Shahan, "Fundamentals of Azure – Microsoft Azure Essentials", Microsoft Press, 2015.**
2. **Michael W, "Implementing Microsoft Azure Infrastructure Solutions", Phi Learning Pvt Ltd, 2009**

Information Security Emerging Trends

L	T	P	C
3	1	0	4

Recommended Prerequisite – None   **Co-requisite** - None

Unit I: Emerging trends in Security

Importance of Security, protecting ever-growing information in e-commerce and m-commerce society, Internet of Everything, End Point Protection, techniques and tools, Security and its economic consequences, case studies, cyber security risk management, emergence of security for Cloud and Big Data, introduction to

28

latest innovations on Security – Microservices and containers unlocking security automation and scalability, data instrumentation delivering better security context, advanced analytics and machine learning enhancing detection capabilities[8]

Unit II: Security Threat Intelligence
Emerging security threat landscape, importance of security threat intelligence, common indicators of compromise, Advanced Persistent Threats (APT), criteria, lifecycle, anatomy of APT, symptoms of APT and countermeasures, network centric warfare, cyber bullying, cyber terrorism, hactivists, process automation[8]

Unit III: Security Incident Response and Malware Analysis
Security incident response management, process, plan, current trends in malware attacks, malware analysis process, techniques and tools, types of malware analysis and stages involved, case study discussions[8]

Unit IV: Adaptive Security

Introduction to Adaptive Security, its importance and implications, key considerations for adaptive security architecture, its role in managing emerging security threats and attacks, averting ripple effect caused by attacks, Security Information and Event Management (SIEM), Digital Right Management (DRM), Digital Loss Prevention (DLP)[8]

Unit V: Cyber Security Framework – Indian Context

Understanding National Cyber Security Policy, DSCI (Data Security Council of India) Security Framework, Overview of RBI Guidelines on Cyber Security Framework, case study on latest data breaches in India and lessons learnt[8]

.
Reference Books:
1. Information Systems Security: Security Management, Metrics, Frameworks and Best Practices by Nina Godbole, Wiley, 1st ed; 2008
2. Cyber Security by Nina Godbole, SModuleBelapure, Wiley, 2011
3. Cybersecurity: Issues of Today, a Path for Tomorrow by Daniel Reis, Archway Publishing (8 Sep 2016)
4. Windows Malware Analysis Essentials by Victor Marak, Packt Publishing Limited (31 August 2015)
5. Cuckoo Malware Analysis by Digit Oktavianto, Iqbal Muhardianto, Packt Publishing Limited (20 September 2013)
6. Tools and Techniques for Fighting Malicious Code: Malware Analyst's Cookbook by Michael Hale Ligh, Steven Adair, Blake Hartstein, Matthew Richard, Wiley (2010)
7. Defensive Security Handbook: Best Practices for Securing Infrastructure by Lee Brotherston, Amanda Berlin, Shroff/O'Reilly; First edition (2017)
8. Threat Modeling: Designing for Security (MISL-WILEY) by Adam Shostack, Wiley, 2014

Cyber Security Incident Response Management

L	T	P	C
3	1	0	4

Recommended Prerequisite – None   **Co-requisite** - None

Unit I: Need for CSIRM

Differences between an event, incident and disaster, what are cyber security incidents, need for CSIRM, policy, plan and procedure, importance of communication protocol, key internal and external stakeholders, law enforcement, role of media, team structure and roles – important considerations[7]

Unit II: Handling a Cyber Security Incident

Incident response lifecycle, incident handling infrastructure and facilities requirements, detection and analysis, process, tools and techniques, attack vectors, recognizing signs of an incident, precursors, indicators and historical organization data, incident correlation, review of logs and vital system parameters, incident handling checklist, documentation and reporting[9]

Unit III: Recovering from Cyber Security Incidents

Nature of incidents and the type of resources it affects, assessment of an incident's impact on business, IT operations and information, determining the amount of time and resources needed in recovering from an incident, prioritization, incident notification structure, containment, eradication and recovery – choosing a containment strategy, evidence gathering and handling, identifying the attack hosts, eradication and recovery, post-incident analysis, evidence retention and lessons learned[9]

Unit IV: Preventing Cyber Security Incidents

Incident analytics as input to proactive security measures to prevent incidents, risk assessment, host security, network security, malware prevention, user awareness and training, analysis of cost of control versus cost of incident impact, best practices[8]

Unit V: Cyber Security Incidents Analysis through Scenarios

Flow chart of scenario questions, scenarios – DoS attack on DNS server, worm and DDoS agent infestation, military-classified documents stolen by an insider, compromised database server, unauthorized access to payroll records, identities and credentials stolen by hackers, antisocial propaganda in media through

30

compromised home wifi network, personal files stored in Cloud are compromised, remote hacking of smart home network, malware infection in home and office network simultaneously, large scale of citizens' biometric data stolen by cyber war groups[7]

.
Reference Books:

1. NIST SP 800-61r2 – Computer Security Incident Handling Guide
2. Computer Incident Response and Product Security (Networking Technology: Security) by DamirRajnovic 1st, Kindle Edition
3. Intelligence-Driven Incident Response: Outwitting the Adversary 1st Kindle Edition
4. The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk by N.K. Mccarthy, Matthew Todd, Jeff Klaben, McGraw-Hill Education, 2012
5. Tools and Techniques for Fighting Malicious Code: Malware Analyst's Cookbook by Michael Hale Ligh, Steven Adair, Blake Hartstein, Matthew Richard, Wiley, 2010
6. Incident Response: A Strategic Guide to Handling System and Network Security Breaches by E. Eugene Schultz, Russell Shumway, Sams, 2001
7. The Effective Incident Response Team by Julie Lucas, Brian Moeller, Addison Wesley, 2003
8. Information Security: Incident Response and Disaster Recovery by Michael E. Whitman, Herbert Mattford, Cengage Learning India Pvt Ltd, 2009
9. Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan 1st Kindle Edition by Jeff Bollinger, Brandon Enright, Matthew Valites, 2015
10. Incident Management and Response Guide: Tools, Techniques, Planning, and Templates Kindle Edition by Tom Olzak, Erudio Security, 2017
11. Cyber Security by Nina Godbole, SunitBelapure, Wiley, 2011
12. Incident Response & Computer Forensics by Jason T. Luttgens, Matthew Pepe, Kevin Mandia, McGraw-Hill Education; 3rd edition, 2014
13. Principles of Incident Response and Disaster Recovery by Michael Whitman, Herbert MattordDelmar Cengage Learning; 2nd Revised edition, 2013
14. Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response by Leighton Johnson, Syngress, 2013
15. Cyber Incident Response: Bridging the Gap Between Cybersecurity and Emergency Management by Response, and Communications and the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security House of Representatives Subcommittee on Emergency Preparedness, CreateSpace Independent Publishing Platform (8 May 2014)

31

Application Security

L	T	P	C
3	1	0	4

Recommended Prerequisite – None   **Co-requisite** - None

Unit I: Phases in Software Development Life Cycle
System Development & Management of Development, Life-Cycle Phases including Project Initiation, Functional Design analysis & Planning, System Design specifications, Software development, Installation and Implementation, Operational Maintenance and Disposal, Separation of duties in the application development lifecycle in the development, testing and Production environments.[8]

Unit II: Introduction to Web Security
Different environments demand different security, Environment versus Application controls, Complexity of Functionality, Data Types, formats and Length, Implementation and Default Issues, Failure states, common web security vulnerabilities, OWASP top 10 threats and counter measures.[7]

Unit III: Features of Java and its Security
Enterprise Java Beans, Expert Systems and Knowledge-Based Systems, Artificial Neural Networks, Object code versus Machine code, Features of Java, Java Security, Active X and Component Object Model (COM), Security issues resulting from Logic Bombs, Malware & Trojan Horses and their impact on Applications[8]

Unit IV: Web application vulnerabilities, attacks and mitigation
Introduction to Web application vulnerabilities and attacks, URL Interpretation attacks, Authentication vulnerabilities, Authorization vulnerabilities, Application Coding vulnerabilities, Input Validation attacks, SQL Injection attacks, Impersonation attacks & Buffer Overflow attacks, their effects and the technical & managerial mitigation controls; overview of automated tools for web vulnerability scanning[8]

Unit V: Current trends in Web Application Security
Clickjacking; DNS rebinding; Flash security; Java applet security; Single-sign-on solution and security; IPv6 impact on web security – importance for IoT; XML security; AJAX attack trends and defense[9]

.

32

Reference Books:
1. Information Systems Security: Security Management, Metrics, Frameworks and Best Practices by Nina Godbole, Wiley, 1sted; 2008
2. Web Application Security, A Beginner's Guide by Bryan Sullivan and Vincent Liu, McGraw Hill; 1sted; 2012
3. HACKING EXPOSED WEB APPLICATIONS by Joel Scambray, McGraw Hill; 3rded; 2010..

4. Web Application Defender′s Cookbook: Battling Hackers and Protecting Users by Ryan C. Barnett and Jeremiah Grossman, John Wiley & Sons, 1sted; 2012
5. The Tangled Web – A Guide to Securing Modern Web Applications by Michal Zalewski, No Starch Press; 1 ed; 2011

Infrastructure Solutions on Cloud Lab

L	T	P	C
0	0	2	1

Recommended Prerequisite –Infrastructure Solutions on CloudCo-requisite - None

List of Programs:

1. Create and document the process of creating a windows azure account
2. Create a virtual machine from available releases of windows server images
3. Create a virtual machine using the option "quick Create"
4. Create a custom VM and Capture the image
5. Create a vm from a captured image
6. Add a VMs to a cluster and deploy load balancer on the same
7. Create and publish / host a webpage in windows azure
8. Create a website using Visual studio
9. Create a SQL server DB , Create tables and add data to the table
10. Test basic sql commands on the table created in the previous step.
11. Migrate an on premise DB to Azure
12. Create a storage account in Azure

Principles of Virtualization Lab

L	T	P	C
0	0	2	1

Recommended Prerequisite –Principles of Virtualization**Co-requisite** - None

List of Programs:

1. Installing VMware ESXi server.
2. Accessing ESXi through vSphere Client and Uploading ISO Images of OS into the Datastore of ESXi Server.
3. Creating Virtual machines in the ESXi Server
4. Monitoring the performance of ESXi Server.
5. Preparing Domain for vCenter Server as prerequisite.
6. Installing vCenter Server
7. Creating Datacenter and adding ESXi Server as Host to vCenter Server.
8. Cloning a Virtual Machine and Creating a Virtual Machine from cloned VM Template.
9. Configuring vNetwork Distributed Switch using vCenter Server.
10. Assigning permissions to users on Datacenter

Mini Project-I

L	T	P	C
0	0	2	1

Recommended Prerequisite – None   **Co-requisite** - None

The students will undertake a project as part of their Sixth semester. The students can do independent projects or can take up projects in groups of two or more depending on the complexity of the project. The maximum group size will be four and in case of team projects there should be a clear delineation of the responsibilities and work done by each project member. The projects must be approved by the mentor assigned to the student. The mentors will counsel the students for choosing the topic for the projects and together they will come up with the objectives and the process of the project. From there, the student takes over and works on the project.

Project Evaluation Guidelines:

The Project evaluator(s) verify and validate the information presented in the project report.

The break-up of marks would be as follows:

1. Internal Evaluation

2. External Assessment

3. Viva Voce

Cyber Forensics & Investigation

L	T	P	C
3	1	0	4

Recommended Prerequisite – None

Co-requisite - None

Unit I: Computer Forensics
Introduction to Computer Forensics, Forms of Cyber Crime, First Responder Procedure- Non-technical staff, Technical Staff, Forensics Expert and Computer Investigation procedure, Case Studies.[8]

Unit II: Storage Devices & Data Recover Methods
Storage Devices- Magnetic Medium, Non-magnetic medium and Optical Medium, Working of Storage devices-Platter, Head assembly, spindle motor, Data Acquisition, Data deletion and data recovery method and techniques, volatile data analysis, Case Studies.[8]

Unit III: Forensics Techniques

Windows forensic, Linux Forensics, Network forensics – sources of network-based evidence, other basic technical fundamentals, Mobile Forensics – data extraction & analysis, Steganography, Password cracking-Brute force, Cross-drive analysis, Live analysis, deleted files, stochastic forensics, Dictionary attack, Rainbow attack, Email Tacking – Header option of SMTP, POP3, IMAP, examining browsers, Case Studies[9]

Unit IV: Cyber Law
Corporate espionage, digital evidences handling procedure, Chain of custody, Main features of Indian IT Act 2008 (Amendment), Case Studies, Incident specific procedures – virus and worm incidents, Hacker incidents, Social incidents, physical incident, Guidelines for writing forensic report.[7]

Unit V: Forensic Analysis of Web Application
Forensic analysis of web server, network analysis of web server compromise, web server log analysis, web application forensic, forensic analysis of web application security, intruder profiling, forensic for code injection attack, Case Studies[8]

.

Reference Books:
1. Computer Forensics: Computer Crime Scene Investigation by John Vacca, Laxmi Publications, 1st ed; 2015

36

2. Digital Forensic: The Fascinating World of Digital Evidences by Nilakshi Jain, et.al, Wiley, 1st ed; 2016
3. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics by John Sammons, Syngress, 2nd ed; 2014
4. Cyber Forensics in India: A Legal Perspective by Nishesh Sharma, Universal Law Publishing - an imprint of LexisNexis; First 2017 edition
5. Network Forensics:Tracking Hackers Throu by Davidoff, Pearson India, 1st ed; 2013
6. Hacking Exposed Computer Forensics by Aaron Philipp, David Cowen, McGraw Hill, 2nd ed; 2009
7. Mastering Mobile Forensics by SoufianeTahiri, Packt Publishing, 1st ed; 2016
8. Computer Forensics: A Beginners Guide by David Cowen, McGraw Hill, 1st ed; 2013
9. Practical Digital Forensics Kindle Edition by Richard Boddington, Packt Publishing, 1st ed; July 2016.
10. Learning Network Forensics by Samir Datt, Packt Publishing, 1st ed; 2016.

Cloud Web Services

L	T	P	C
3	1	0	4

Recommended Prerequisite – None   **Co-requisite** - None

Unit I: Introduction to Cloud Computing and Amazon Web Services
Introduction to Cloud Computing, Cloud Service Delivery Models (IAAS, PAAS, SAAS), Cloud Deployment Models (Private, Public, Hybrid and Community), Cloud Computing Security, Case Study.
Introduction to Amazon Web Services, Why Amazon? Use Cases, AWS Storage Options, AWS Compute Options, AWS Database Options, AWS Workflow Automation and Orchestration Options, AWS Systems Management And Monitoring Options, AWS Virtual Private Cloud Introduction, Pricing Concepts.[8]

Unit II: Introduction to EC2
Introduction To EC2, Instance Types And Uses, Auto scaling Instances, Amazon Machine Images (AMIS), Modifying Existing Images, Creating New Images of Running Instances, Converting An Instance Store AMI To An EBS AMI, Instances Backed By Storage Types, Elastic IPS, Elastic Load Balancing[7]
.
Unit III: Web Applications And Security

Introduction to Elastic Beanstalk, Deploying Scalable Application On AWS, Selecting And Launching An Application Environment, Provisioning Application Resources with Cloud formation, Introduction to CloudWatch, Describe Amazon Cloud Watch metrics and alarms, AWS Messaging Services(SNS,SQS,SES). Introduction to AWS Security, Describe Amazon Identity and Access Management (IAM), AWS Directory Service, AWS Key Management Service, Securing Data at Rest and In Motion[9]

Unit IV: AWS Storage
Amazon Storage, S3 Storage Basics, Buckets and Objects, Creating A Web Server Using S3 Endpoints, Managing Voluminous Information with EBS, Glacier Storage Service , Describe Amazon Dynamo, Understand key aspects of Amazon RDS, Launch an Amazon RDS instance.[8]

Unit V: AWS Networking
Introduction to AWS Networking , Access Control Lists (ACLs), Setting Up a Security Group, Setting Up VPC And Internet Gateway, Setting Up A VPN, Setting Up A Customer Gateway For VPN, Setting Up Dedicated Hardware For VPC, Scenario 1:VPC With A Public Subnet Only (Standalone Web), Scenario 2: VPC with Public And Private Subnets (3 Tier App), Scenario 3:VPC With Public And Private Subnets And Hardware VPN Access (Web On The Cloud, Database and App On Prem) Scenario 4: VPC With A Private Subnet Only And Hardware VPN Access. (Extension Of Your Corporate Network), Route53 for DNS System, Cloud front, Case Study[8]
.

Reference Books:
1. **Joe Baron, HishamBaz , Tim Bixler , Biff Gaut , Kevin E. Kelly , Sean Senior , John Stamper , "AWS Certified Solutions Architect Official Study Guide: Associate Exam, John Wiley and Sons Publications, 2017**
2. **YohanWadia , "AWS Certified Solutions Architect Official Study Guide: Associate Exam, John Packt Publishing, 2016**
3. **Bernald Golden, "Amazon Web Services for Dummies", John Wiley & Sons, 2013**

Linux Administration

L	T	P	C
2	1	0	3

Recommended Prerequisite –None   **Co-requisite** - None

Unit I: Introduction to Linux
Introduction to Operating system - Types of Operating system - Multi user operating system - Open source licensing - History of Linux - Unix Vs Linux - Flavors of Linux - Benefits and characteristics of Linux - Installation of Linux - Linux booting process - Log in and switch users in multiuser run levels - Shell and bash features - Linux kernel - sudovssu - Date and time configuration – Linux run levels

Directories and files : Directory structure - System directory - Absolute path and relative path -Creating and removing directory - Changing directory path - Creating - removing - copying and moving files - File Permissions - Links – hard link and soft link - Input and output redirection - Filters and pipes - Locate - read - and use system documentation including man page[9]

Unit II: Package, User and group Management
RPM - YUM - Archive - Compress - unpack and uncompress files using tar - star - gzip - and bzip2 - Create - delete - and modify local user accounts - Change passwords for local user accounts - Create - delete - and modify local groups and group memberships - Changing owner and modes[6]

Unit III: Configuring local storage and filesystem
List - create - delete - and partition type for primary - extended - and logical partitions -   Create and remove physical volumes - assign physical volumes to volume groups - Create and delete logical Volumes. - Create - mount - unmount - ext2 - ext3 - and ext4 file systems. - Mount - unmount - and LUKS-encrypted file systems - Access control list[7]

Unit IV: Managing system and infrastructure services
Managing system services - Shutting down - suspending and hibernating the system - Controlling systemd on remote machine - Creating and modifying systemd unit files – DHCP Configuration - HTTP server Configuration - FTP server Configuration - Mail server Configuration - Samba server Configuration - NTP server Configuration - NFS server Configuration [7]

Unit V: OpenSSH and Linux security
OPENSSH - The SSH Protocol - Configuring OpenSSH and Starting an OpenSSH Server Key-Based Authentication in OpenSSH - OpenSSH Clients - Using the ssh Utility - scp Utility and sftp Utility - Configure firewall settings using system-config-firewall or iptables - Set enforcing and permissive modes for SELinux - List and identify SELinux file and process context.[6]

Reference Books:
1. **Orsaria, Jang, "RHCSA/RHCE Red Hat Linux Certification Study Guide Exams EX200 & EX300", McGraw-Hill Education, July 2017.**
2. **Sander Van Vugt, "Red Hat RHCSA/RHCE 7 Cert Guide: Red Hat Enterprise Linux 7 (EX200 and EX300)", Phi Learning Pvt Ltd, 2009.**

Disaster Recovery and Business Continuity Management

L	T	P	C
2	1	0	3

Recommended Prerequisite –None**Co-requisite** - None

Unit I: Business Continuity Management
Introduction to Business Continuity Planning (BCP), Business Resumption Plan (BRP) or Disaster Recovery Plan (DRP), Common terminologies used in BCP and DRP, Business Continuity Management (BCM), NIST SP800-34 Emergency Action plan which includes the phases of Recover/Resume, Protect and Sustain, Causes of Disasters.[8]

Unit II: Stages in BCP
BCP objectives. Information Protection Environment. Security Technology and Tools. Steps involved in creating a BCP, Phase 1: Project Management and Initiation. Phase 2: Business Impact Analysis. Phase 3: Recovery Strategies, Phase 4: Plan Development and Implementation.[8]

Unit III: Business Recovery strategies
Facility and Supply Recovery strategies. User Recovery strategies. Technical Recovery strategies, Data Recovery strategies, Activation Phase- Major Disaster or Disruption, Intermediate Disaster or Disruption, Minor Disaster, Activating BC/DR Teams, Developing Triggers, Transition Trigger. Defining BC/DR Team and Key Personnel, Defining Tasks, Assigning Resources, Communication Plan.[7]

Unit IV: Testing, Maintenance, Awareness & Training Mechanisms
Different types of tests including structured walk-through, checklist test, simulation, parallel test and full interruption test. Steps required to maintain a BCP. [6]

Unit V: Preparation of BCP
Requirements for BCP awareness and training, Conduct a case study of IT Organization and prepare a Business Continuity Plan for the same using the learning from this course.[6]

Reference Books:

1. Business Continuity and Disaster Recovery Planning for IT Professionals by Susan Snedaker, Syngress; 2 edition (31 October 2013)

2. Business Continuity and Disaster Recovery Planning by Stuart Hotchkiss, BCS, The Chartered Institute for IT, 1sted; 2011

3. Information Systems Security: Security Management, Metrics, Frameworks and Best Practices by Nina Godbole, Wiley, 1st ed; 2008

4. Planning for Disaster: A Business Survival Guide by Harry Flowers, CreateSpace Independent Publishing Platform; 1 edition (15 August 2015)

5. Disaster Management: How to Conduct Business Continuity and Disaster Recovery During Disaster Planning, Response and Recovery: 3 (Disaster Management How To Series) by Ian Watts, CreateSpace Independent Publishing Platform; 1 edition (28 November 2016)

6. Simple Guidelines for Successful Disaster Recovery Planning: What are the steps to create an emergency response plan, and how would you utilize this plan by Harry R Fisher, CreateSpace Independent Publishing Platform (27 January 2015)

7. Business Continuity from Preparedness to Recovery: A Standards-Based Approach by Eugene Tucker, Butterworth-Heinemann; 1 edition (5 January 2015)

Exchange Server Administration

L	T	P	C
3	1	0	4

Recommended Prerequisite –None   **Co-requisite** - None

Unit I: Putting Exchange Server 2013 into context, Introducing Change in Exchange Server 2013
Significance of e-mail communication: Importance of Email, Messaging Services, Exchange Server, Many modes of access, The Universal Inbox, Architecture Overview. Controlling Mailbox growth, Personal folders or PST files, Email archiving, Public Folders, Things every Email-administrators should know, Tools. Exchange Server 2013: Getting to know Exchange Server 2013, Exchange Server Architecture, x64 processor requirement, Windows Server 2008 R2 and Widows Server 2012 Installer, Service Pack and Patching Improvements Server roles, Edge Transport Services, Unified Messaging and Client Connectivity. The managed store, High-Availability Features Content Storage, Exchange Server Management, Improved Message and Content Control, Built-in Archiving, Message Transport Rules, Message Classifications, Rights Management, Service Message Protection Programming Interfaces, New and Improved Outlook Web App, Mobile Clients and Improved Security.[8]

41

Unit II: Understanding Availability, Recovery, Compliance, and Virtualization Server Exchange 2013:
What's in a Name, Backup and Recovery, Disaster Recovery, Management Frameworks, A Closer Look at Availability, Storage Availability , An Overview of Exchange Storage, Direct Attached Storage, Storage Area Networks, Compliance and Governance, The Bottom Line. Virtualization Overview, Understanding Virtualized Exchange, Understanding Your Exchange Environment Effects of Virtualization, Environmental Impact, Space Impact, Complexity Impact, Additional Considerations, Virtualization Requirements, Hardware Requirements, Software Requirements, Operations, Deciding What to Virtualized, Exchange Roles ,Testing, Possible Virtualization Scenarios, Small Office/Remote or Branch Office , Site Resilience, Mobile Access[9]

Unit III: Introducing Power Shell, Exchange Management Shell and Getting Exchange Server Running
Why Use Power Shell, Understanding the Command Syntax, Verbs and Nouns, The -Identity Parameter, Cmdlet Parameters, Alias, Object-oriented Use of Power Shell, Filtering Output, Formatting Output, Directing Output to Other Cmdlets, Power Shell v3 , Remote Power Shell, Tips and Tricks, Managing Output, Running Scripts, Running Scheduled Power Shell Scripts, Debugging and Troubleshooting from Power Shell, Auto discover Concepts, What Auto discover Provides , How Auto discover Works. Hardware, Operating Systems, Configuring Windows, Understanding Server Role and Configuration, Active Directory Requirements, Installing Exchange Server 2013, GUI-based Installation, Command-line Installation, Post-installation Configuration Steps, Final Configuration.[9]

Unit IV: Understanding Server roles, configuration, Exchange server 2013 requirement and Installation
Server Roles, exchange server 2013 server roles, mailbox server, client access server, possible role configurations, combined-function server, scaling exchange server 2013 roles. Selecting the right server hardware, the typical user, CPU recommendations, memory recommendations, network recommendations, disk recommendations, software recommendations, operating recommendations, windows 7/windows 8 management consoles, additional requirement, active directory requirement, installation and preparation permissions.[7]

Unit V: Introducing Power Shell and Exchange Management Shell
Why Use Power Shell, Understanding the Command Syntax, Verbs and Nouns, The -Identity Parameter, Camlet Parameters, Alias, Object-oriented Use of Power Shell, Filtering Output, Formatting Output, Directing Output to Other Camlets, Power Shell v3 , Remote Power Shell, Tips and Tricks, Managing Output, Running Scripts, Running Scheduled Power Shell Scripts, Debugging and Troubleshooting from Power Shell, Auto discover Concepts, What Auto discover Provides , how Auto discover Works.
Getting Exchange Server Running.   Hardware, Operating Systems, Configuring Windows, Understanding Server Role and Configuration,
Active Directory Requirements, Installing Exchange Server 2013, GUI-based Installation, Command-line Installation, Post-installation Configuration Steps, Final Configuration[7]
.

Reference Books:
1. Mastering Exchange server 2013 by David Elfassy
2. "Microsoft Exchange Server 2013 Unleashed " By Rand Morimoto, Michael Noel, Guy Yardeni, Chris Amaris, Andrew Abbate, Technical Edit by Ed Crowley, 2012 edition.

Advance Virtualization

L	T	P	C
3	1	0	4

Recommended Prerequisite – Principles of Virtualization   **Co-requisite** - None

Unit I: Security Concepts
Role Based Access Control(RBAC), Explicit Permissions, Managing User and Group Lists, Server Roles and Directory Services, Harden Virtual Machine, ESXi Hosts and vCenter Server, SSO Architecture and Components, Various Authentication Methods, SSO – Users, Installation and Policies[8]

Unit II: Storage
Storage LUNs, Configure LUNs, NFS Share, iSCSI initiator – Software, Hardware, Configure iSCSI initiator, Editing initiator Settings, Port binding, VSAN and VVOL architectural components, Managing Virtual SAN and Virtual Volumes, Storage Policies, Storage I/O Control.[8]

Unit III: Networking
Networking: Create, configure, and manage vNetwork standard switches, Create, configure, and manage network connections, Create, configure, and manage port groups, Storage: Configure ESX/ESXi with iSCSI, NFS, Create and manage vSphere data stores.[8]

Unit IV: Virtual Machines
Virtual Machines: Deploy virtual machines using VMware vCenter Converter, Resource Monitoring, Control virtual machine access to CPU, memory, and I/O resources, Introduce VM kernel methods for optimizing CPU and memory usage Monitor resource usage using vCenter Server performance graphs and alarms, Data Protection: Back up and recover virtual machines using VMware Data Recovery.[8]
.
Unit V: Scalability

Manage multiple vCenter Server inventories using VMware vCenter Linked Mode, Manage ESX/ESXi configuration compliance using Host Profiles, Create, configure, and manage vNetwork distributed switches, network connections, and port groups, Configure and manage a VMware Distributed Resource Scheduler cluster High Availability, Configure and manage a VMware High Availability cluster, Configure fault-tolerant virtual machines using VMware Fault Tolerance, Patch Management: Manage patching and patch compliance using vCenter Update Manager[8]

Reference Books:
1. John A. Davis, Steve Baca, Owen Thomas, "VCP6-DCV Official Cert Guide (Exam #2V0-621)", 3rd Edition, VMware Press.
2. "Nick Marshal, "Mastering VMware vSphere 6", 1st Edition, Wiley Publications

Infrastructure Automation

L	T	P	C
3	1	0	4

Recommended Prerequisite – None   **Co-requisite** - None

Unit I: Introduction to Chef

Idempotency/convergence - test & repair model - Common resources and their actions- Default actions- The ':nothing' action - The 'supports' directive - The 'not_if' and 'only_if' directives - Resource extensibility -RECIPES: What a recipe is - Importance of the resource order - How to use 'include_recipe' - What happens if a recipe is included multiple times in a run_list - The 'notifies' and 'subscribes' directives [8]

Unit II: COOKBOOKS and chef server

Cookbook contents - Naming conventions - Cookbook dependencies - The default recipe - How the Chef server acts as an artifact repository - How the Chef server acts as an index of node data - Chef solo vs Chef server - Chef server's distributed architecture - Scalability [7]

44

Unit III: Chef client

The function of Chef client vs the function of Chef server - What 'why-run' is - How to use '--local-mode' - How the Chef client and the Chef server communicate - The Chef client configuration - What a node is - What a node object is - How a node object is stored on Chef server - How to manage nodes - How to query nodes - How to name nodes[8]

Unit IV: Puppet infrastructure & Resource and manifests

Introduction To Configuration Management - Importance of puppet - How To Access Your Working Files - Puppet Agents - Puppet Masters Systems Orchestration - Cross Platform Puppet. Introduction To Puppet Run Cycle - Gathering System Facts - Node Matching And Catalogue Compilation - Puppet Resources - How To Define System Resources - Applying A Simple Puppet Manifest - Puppet Types - The Package File Service Pattern - Applying Conditional - - Logic In Puppet - Fact Conditionals - Choosing A Course Of Action.[9]

Unit V: Puppet Environment and MCollective

Defining Nodes - Puppet Modules - Reusable Code - Forge Modules - Where To Find Reusable Code - Provisioning A Web Server - Class Parameters - Applying Variables - Hiera Parameters - Defining Variables - Executing Modules Against A Puppet Master With An Agent - Reporting With Puppet - MCollective And Live Management - MCollective With Puppet - Using MCollective To Interact With Services - Using MCollective To Interact With Puppet[8]

Reference Books:
1. Managing Infrastructure with Puppet Paperback – 29 Jun 2011 by James Loope
2. Chef Cookbook Paperback – Import, 3 Feb 2017 by Matthias Marschall (Author)
3. DevOps for Beginners: Hands-on Guide Kindle Edition by David Johnson– 2016 edtion

IT Governance, Risk and Information Security Management

L	T	P	C
3	1	0	4

Recommended Prerequisite – None **Co-requisite** - None

Unit I: IT Governance-Part 1

Introduction & Concepts, Origin of Governance, Corporate Governance, Best Practices for IT Governance, Role of Governance in Information Security, Six outcomes of effective Security Governance, benefits of good governance, Cultural aspects in governance.[8]

Unit II: IT Governance-Part 2
ITGovernance-Roles and Responsibilities, Role of IT Strategy Committee and Security Steering Committee, Standard IT Balanced Scorecard. Val-IT framework of ISACA, Governance in multi-department and multi-country enterprises, Importance of Governance in establishing a sustainable Security Culture in the organization.[8]

Unit III: Information Systems Strategy
Role of Strategic Planning for IT, Strategic Direction and Alignment of Security Strategy with Business Objectives, Role of CISO, Security Metrics Program.[8]

Unit IV: Risk Management Program
Develop a Risk Management Program. Risk Management Process, Roles and Responsibilities, Risk-IT Framework of ISACA, Strategic Security decisioning using Risk Management, [8]

Unit V: Information Security Management
Introduction, Performance Optimization, Management Information Security Forum, Segregation of Duties, Description of COBIT and other Frameworks, Security Program Effectiveness, Continuous Assessment and Improvement, In-sourcing versus Out-sourcing, Impact of ISM program across organization.[8]

Reference Books:
1. Information Security Governance by S.H. Solms, RossouwSolms, Springer; 1st Edition. 2nd Printing, 2008 edition (12 December 2008)
2. IT Governance: How Top Performers Manage IT Decision Rights for Superior Results by Weill, Harvard Business Review Press; First edition (1 June 2004).
3. ISACA publications.
4. Managing Risk and Information Security by Malcolm Harkins, Apress; 1 edition, 2012
5. IT Governance: An International Guide to Data Security and ISO27001/ISO27002 by Alan Calder, Steve Watkins, Kogan Page; 6 edition (3 September 2015)
6. ISACA publications on COBIT, RiskIT and ValIT
7. Information Security Governance: Guidance for Information Security Managers by W. KragBrotby and IT Governance Institute, Isaca (2 June 2008)
8. COBIT 5 Framework Perfect by Isaca, (10 April 2012)
9. Cobit 5 Foundation-reference and Study Guide by Ana Cecilia Delgado, CreateSpace Independent Publishing Platform; Stg edition (20 June 2016)

10. Governance of Enterprise IT Based on COBIT 5: A Management Guide by Geoff Harmer (Author), IT Governance Publishing, (6 February 2014)

COBIT VALIT RISKIT

L	T	P	C
3	1	0	4

Recommended Prerequisite – None   **Co-requisite** - None

Unit I: Introduction to COBIT
COBIT 5 – Its importance and relevance - 5 Principles of COBIT

   a) Meeting Stakeholders needs

   b) Covering the Enterprise End-to-End

   c) Applying a Single Integrated Framework

   d) Enabling a Holistic approach

   e) Separating the Governance from the Management

Enablers of COBIT
   a) Processes

   b) Organizational Structures

   c) Culture, Ethics &Behaviour

   d) Principles, Policies & Frameworks

   e) Information

   f) Services Infrastructure Applications

   g) People, Skills & Competencies. [10]

Unit II: Risk IT and Val IT – Importance and Relevance for Information Security

Interlinkages between Risk IT with COBIT & Val IT, three domains of Risk IT with their sub processes

Risk Governance

    a) Establish and Maintain a Common Risk view

    b) Integrate with Enterprise Risk Management (ERM)

    c) Make Risk-aware Business Decisions

Risk Evaluation
    a) Collect data

    b) Analyze Risk

    c) Maintain Risk Profile

Risk Response
    a) Articulate Risk, Manage Risk, React to Events

ValIT, its importance and relevance, key ValIT terms, principles and domains [9]

Unit III: Introduction to Information Security Governance (ISG)
Importance of ISG, Benefits of ISG, monitoring ISG through metrics, approach for implementing ISG, how ISG it connected to ITG and Corporate Governance [7]

Unit IV: Applying COBIT 5 principles, RiskIT, ValIT in Information Security Governance
How the Principles and Processes are connected to ISG, applying the principles in ISG, separating governance and management in ISG, benefits.[7]

Unit V: Framework on ISG

Overview of ISO/IEC 27014:2013 Information technology — Security techniques — Governance of information security, How ISG impacts Cloud, Mobile, Big Data, Analytics and AI? Case Studies on Corporate Governance, IT Governances and Information Security Governance.[7]

Reference Books:
    1. Information Security Governance by S.H. Solms, RossouwSolms, Springer; 1st Edition. 2nd Printing, 2008 edition (12 December 2008)

2. IT Governance: How Top Performers Manage IT Decision Rights for Superior Results by Weill, Harvard Business Review Press; First edition (1 June 2004)
3. ISACA publications
4. IT Governance: An International Guide to Data Security and ISO27001/ISO27002 by Alan Calder, Steve Watkins, Kogan Page; 6 edition (3 September 2015)
5. ISACA publications on COBIT, RiskIT and ValIT
6. Information Security Governance: Guidance for Information Security Managers by W. KragBrotby and IT Governance Institute, Isaca (2 June 2008)
7. COBIT 5 Framework Perfect by Isaca, (10 April 2012)
8. Cobit 5 Foundation-reference and Study Guide by Ana Cecilia Delgado, CreateSpace Independent Publishing Platform; Stg edition (20 June 2016)
9. Governance of Enterprise IT Based on COBIT 5: A Management Guide by Geoff Harmer (Author), IT Governance Publishing, (6 February 2014)

ISO 27001, PCI DSS & HIPAA

L	T	P	C
3	1	0	4

Recommended Prerequisite –Co-requisite - None

Unit I: ISO 27001
Auditing: Principles of auditing, Conducting and Managing an Audit Program. Auditing Activities: Scoping and Pre audit Survey, Planning and preparation, Fieldwork, Analysis, Reporting, Closure, Competence and evaluation of auditors: Auditor competence, Information Security Management System Audit Testing: Information security management system, Management responsibility, Internal ISMS audits, Management review of the ISMS, ISMS improvement [8]

Unit II: Information Security Audit Check Listing
Security Policy, Organizing information security, Asset management, Human resources security, Physical and environmental security, Communications and operations management, Access control, Information systems acquisition, development and maintenance, Information security incident management, Business continuity management, Compliance.[8]

Unit III: PCI DSS

Scope of PCI DSS Requirements, Best Practices for Implementing PCI DSS into Business-as-Usual Processes, PCI DSS Assessment Process, PCI DSS Requirements: Build and Maintain a Secure Network and Systems, Protect Cardholder Data, Maintain a Vulnerability Management Program, Implement Strong Access Control Measures , Regularly Monitor and Test Networks, Maintain an Information Security Policy.[8]

Unit IV: HIPAA - Purpose and Scope
HIPAA Security Rule, Security Rule Goals and Objective, Security Rule Organization, Administrative Safeguards: Security Management Process, Assigned Security Responsibility, Workforce Security, Information Access Management, Security Awareness and Training, Security Incident Procedures, Contingency Plan, Evaluation, Business Associate Contracts and Other Arrangements.[8]

Unit V: Physical and Technical Safeguards
Physical Safeguards: Facility Access Controls, Workstation Use, Workstation Security, Device and Media Controls, Technical Safeguards: Access Control, Audit Controls, Integrity, Person or Entity Authentication, Transmission Security, Organizational Requirements: Business Associate Contracts or Other Arrangements, Requirements for Group Health Plans.[8]

Reference Books:
1. Information Security Policy Development for Compliance: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0, Barry L. Williams, Auerbach Publications; 1 edition (6 March 2013)
2. Foundations of Information Security Based on ISO27001 and ISO27002 (Best Practice) by Hans Baars et.al., van Haren Publishing; 3rd Revised edition edition (15 April 2015)

Cyber Forensics & Investigation Lab

L	T	P	C
0	0	2	1

Recommended Prerequisite –Cyber Forensics &InvestigationCo-requisite - None

50

List of Programs:

1. Physical Collection of electronic evidence using forensic standards

2. Dismantling and re-building PCs in order to access the storage media safely

3. Boot sequence and Power On Self-Test mode analysis

4. Examination of File systems of Windows, Linux and Mac

5. Analysing Word processing and Graphic file format

6. Network data sniffing and analysing

7. Password and encryption techniques

8. Internet forensic and Malware analysis

9. Data recovery techniques for hard drive

10. Data recovery techniques for Pen drive and CD

Cloud Web Services Lab

L	T	P	C
0	0	2	1

Recommended Prerequisite –Cloud Web ServicesCo-requisite - None

List of Programs:

1. Introduction to Amazon Simple Storage Service (S3)

2. Introduction to Amazon Cloud Front

3. Introduction to AWS Key Management Service

4. Introduction to Amazon Elastic search Service

5. Introduction to Amazon Dynamo DB

6. Introduction to Amazon API Gateway

7. Introduction to Amazon Redshift

8. Introduction to Amazon Aurora

9. Introduction to Amazon Machine Learning

10. Introduction to AWS Database Migration Service

11. Introduction to AWS Lambda

12. Introduction to AWS Internet-of-Things (IoT)

13. Introduction to AWS Device Farm

14. Introduction to Amazon Kinesis Firehose

15. Introduction to Amazon Route 53

16. Introduction to Amazon Elastic File System (EFS)

17. Challenge Lab

Linux Administration Lab

L	T	P	C
0	0	2	1

Recommended Prerequisite–Linux AdministrationCo-requisite - None

List of Programs:

1. Configure the following tasks & verify it. (Hint - use grep/cut/tr/sed)
   - a)   List the lines containing "/sbin/nologin" from the /etc/passwd file.
   - b)   List only lines of output from ps, which lists running processes that contain the string "in
   - c)   Display the list of GIDs from /etc/passwd file.
   - d)   Alter all the letters that starts from range "a-f" to "A-F" in /etc/passwd file.

2.   Create an alias named eth0:0 using below credentials in RHEL 5 and verify it.

(a) IP ADRESS = 172.16.0.1   (b) 255.255.0.0
(c) Default Gateway = 172.16.0.254 (d) DNS 1 = 4.2.2.1

3.   Configure password policy for user john with below arguments in RHEL 5. After configuration verify the policy applied.

(a) Minimum password age = 4 days
(b) Maximum password age = 15 days
(c) Inactive days = 2 days
(d) Account Expiration date = 6 months from today

4   Configure the following tasks:
   (a)   Add user accounts to your system: Joshua, alex, dax, bryan, zak, ed and manager. Assign each user this password: 123@iMs.

   (b)   Add the groups to your system: sales with GID: 1000, HR with GID: 1100 and web with GID: 1200.
   (c)   Add Joshua and alex to the sales group, dax and bryan to the HR group, zak and ed to the web group and add manager to all of these groups.

   (d)   Login with each user & verify using id command that they are in the appropriate groups.
5   Use ACL to accomplish these tasks:
   (a)   Create groups named Admin and Web.
   (b)   Create users named John and Jimmy.
   (c)   Create a new directory named /depts/tech/. Change the permission so that root is the owner and Admin is the group owner.

   (d)   Use ACL to give full permission for /depts/tech/ to the Web group.
   (e)   Allow John read/execute but not write permission on the /depts/tech/ directory.
   (f)   Allow Jimmy full permission on the /depts/tech/ directory.
6   You are tasked with finding all SUID & SGID files under the / directories.

7   Configure your system that boots to run level 3 by default. Configure X server using command in run level 3.

8   Devise a ps command that does the following. (Hint: sort/ps/top)

(a)   List all processes.

(b)   For each process, prints the information which displays the percentage of CPU usage, the process ID & name of the command that created it.

(c)   The output is sorted by the %cpu value from highest to lowest

9   Explain the suid, sgid& sticky bit permission with example

10   Customize the Bash prompt as per given tasks (Hint - PS1)

     (a)   Display the current value of primary prompt string.

     (b)   Changes prompt to print a static string "ITIMS -'".

     (c)   Restore the original prompt.

     (d)   Insert the bash history prompt special character "\!" between the hostname and dollar-sign.

11   Configure given tasks for package management: (Hint: use rpm command)

     (a)   Check whether ftp package is installed or not.

     (b)   If it is not installed, install it & verify it.

     (c)   Display the configuration files available through this package.

     (d)   Be sure that ftp service must be enabled at startup.

12   Use rpm queries to answer the following questions.

     (a)   What files are in the "initscripts" package?

     (b)   Which installed packages have "gnome" in their names?

     (c)   Which RPM provides /etc/inittab?

13.   Prepare a cron job that take the backup of /home at 5:00pm on every Saturday.

14.   Change your system date to 1:00pm March 1990.

Mini Project-II

L	T	P	C
0	0	2	1

Recommended Prerequisite – None   **Co-requisite** - None

The students will undertake a project as part of their seventh semester. The students can do independent projects or can take up projects in groups of two or more depending on the complexity of the project. The maximum group size will be four and in case of team projects there should be a clear delineation of the responsibilities and work done by each project member. The projects must be approved by the mentor assigned to the student. The mentors will counsel the students for choosing the topic for the projects and together they will come up with the objectives and the process of the project. From there, the student takes over and works on the project.

Project Evaluation Guidelines:

The Project evaluator(s) verify and validate the information presented in the project report.

The break-up of marks would be as follows:

1. Internal Evaluation
2. External Assessment
3. Viva Voce

IT Infrastructure Library

L	T	P	C
2	1	0	3

Recommended Prerequisite – None   **Co-requisite** - None

Unit I: ITIL Overview and Service Strategy
ITIL History, Components of the ITIL Library, IT Service Management, Organizing for IT Service Management, Technology and Architecture, Overview of HPSM and OTRS as service management tool, Service Strategy: Service Strategy Lifecycle Stage, Service Portfolio Management, the Demand Management Process, the IT Financial Management Process, Introduction to ISO 20000 Standards [7]

Unit II: Service Design
Service Design Lifecycle Stage, The Service Catalog Management Process, The Service Level Management Process, The Availability Management Process, The Capacity Management Process, The Information Security, Management Process, The IT Service Continuity, Management Process, The Supplier Management Process   [7]

Unit III: Service Transition
Service Transition Lifecycle Stage, the Change Management Process, the Release and Deployment Management Process, the Service Asset and Configuration Management Process, Knowledge Management [6]

Unit IV: Service Operation, Continual Service Improvement
Service Operation Functions: Service Operation Lifecycle Stage, The Service Desk Function, The Technical Management Function, The Application Management Function, The IT Operations Management Function Service Operation Processes: The Event Management Process, The Incident Management Process, The Request Full fillment Process, The Access Management Process, The Problem Management Process, [8]

57

Unit V: Continual Service Improvement
Continual Service Improvement principles - CSI and organizational change,Ownership, Role definitions , External and internal drivers , Service Level Management , The Deming Cycle, Service measurement ,Knowledge Management, Benchmarks , Governance ,Frameworks, models, standards and quality systemsContinual Service Improvement processes : 7step improvement process, Service reporting, Service management, return on in investment for CSI, business questions for CSI, Service level management[7]

Reference Books:

1. Introduction to ITIL, Jan van Bon Stationery Office Books, The Stationery Office, 2010

2. HP operation Manual from HP, 2010

3. A Guide to Service Desk Concepts Donna Knapp From Cengage Learning, 2010

4. The Shortcut Guide to Virtualization and Service Automation, Greg Shield Real-time Publishers, 2008

5. Service automation and dynamic provisioning techniques in IP/MPLS environments - Christian Jacquenet, Gilles Bourdon, Mohamed Boucadair John Wiley and Sons, 2008

B.Tech Project

L	T	P	C
0	0	0	12

Recommended Prerequisite – None   **Co-requisite** - None

The students will undertake a project as part of their final semester. The students can do independent projects or can take up projects in groups of two or more depending on the complexity of the project. The maximum group size will be four and in case of team projects there should be a clear delineation of the responsibilities and work done by each project member. The projects must be approved by the mentor assigned to the student. The mentors will counsel the students for choosing the topic for the projects and together they will come up with the objectives and the process of the project. From there, the student takes over and works on the project.

If the student chooses to undertake an industry project, then the topic should be informed to the mentor, and the student should appear for intermediate valuations. Prior to undertaking this project the students undergo a bridge course.

Bridge Course:

The bridge course ensures that all the students have the correct prerequisite knowledge before their industry interface. The purpose of a bridge course is to prepare for a healthy interaction with industry and to meet their expectations. It would be difficult to establish standards without appropriate backgrounds and therefore to bridge this gap, students are put through a week mandatory classroom participation where faculty and other experts will give adequate inputs in application based subjects, IT and soft skills.

The Project:
Each student will be allotted a Faculty Guide and an Industry Guide during the internship/project work. Students need to maintain a Project Diary and update the project progress, work reports in the project diary. Every student must submit a detailed project report as per the provided template. In the case of team projects, a single copy of these items must be submitted but each team member will be required to submit an individual report detailing their own contribution to the project.
Each student/group should be allotted a supervisor and periodic internal review shall be conducted which is evaluated by panel of examiners.

Project Evaluation Guidelines:

The Project evaluator(s) verify and validate the information presented in the project report.
The break-up of marks would be as follows:
   1. Internal Evaluation
   2. External Assessment
   3. Viva Voce

Internal Evaluation:
Internal Evaluator of project needs to evaluate Internal Project work based on the following criteria:
- Project Scope , Objectives and Deliverables
- Research Work, Understanding of concepts
- Output of Results and Proper Documentation
- Interim Reports and Presentations– Twice during the course of the project

External Evaluation:
The Project evaluator(s) perform the External Assessment based on the following criteria.
- Understanding of the Project Concept

59

- Delivery Skill
- The Final Project Report
- Originality and Novelty

The Final Project Report Details:
- The report should have an excel sheet that documents the work of every project member

Viva Voce
- Handling questions
- Clarity and Communication Skill

Marking Scheme:
1. **Internal Evaluation:** 35% of Total Marks
2. **External Evaluation:** 50% of Total Marks
3. **Viva Voce:** 15 % of Total Marks

For e.g., If the total mark for the project is 100, then
- ❖ Internal Evaluation = 35 marks

The break-up of marks is shown below:-

- Interim Evaluation 1: 10 marks
- Interim Evaluation 2: 10 marks
- Understanding of concepts: 5 marks
- Programming technique: 5 marks
- Execution of code : 5 marks

- ❖ External Evaluation = 50 marks

The break-up of marks is shown below:-

- Project Report: 15 marks
- Explanation of project working: 10 marks
- Execution of code: 10 marks – (if done in industry, a stand-alone module can be reprogrammed and submitted. Error rectification etc. can be included by the evaluator)
- Participation in coding: 15 marks

❖   Viva Voce = 15 marks

The break-up of marks is shown below: -

- Questions related to project: 10 marks
- Questions related to technology: 5 marks

The Project evaluator(s) verifies and validates the information presented in the project report.