Course Competency

CIS 2430C Remote IT and Security Management

Course Description

This course equips students with essential tools and strategies for Remote IT and Security Management (RITSM). It covers proactive security, business continuity, disaster recovery, and the use of Managed Service Provider (MSP) tools. Participants explore RITSM tools and technologies such as RMM, IT Glue, and Datto Networking. Prerequisites: CTS1134 and CTS1120. (3 hr. lecture; 2 hr. lab).

Course Competency	Learning Outcomes
Competency 1: The student will demonstrate an understanding of the fundamentals of Remote IT and Security Management (RITSM) by:	1. Critical thinking 2. Information Literacy 3. Computer / Technology Usage
1. a) Identifying the critical tools leveraged by a managed service provider (MSP) to support proactive security, business continuity, and disaster recovery. b) Listing the seven (7) steps within the IT Complete Journey to support a customer's IT infrastructure. c) Defining the standard functionality of a Remote Monitoring and Management (RMM) tool to manage customer bases. d) Recognizing the operational enhancements gained by leveraging dashboards and entity categories within a business management tool. e) Recognizing key concepts of IT documentation tools such as IT Glue to document technical information and procedures. f) Listing the areas of cloud data responsibility by MSPs and users by leveraging the Shared Responsibility model. g) Describing the fundamentals of email security, endpoint security, and network security to protect against cyber-attacks. h) Listing the fundamental principles of networking solutions that enable MSPs to successfully generate	

recurring revenue.	
Competency 2: The student will demonstrate an understanding of the business aspects of RITSM by:	1. Communication 2. Numbers / Data 3. Critical thinking 4. Information Literacy 5. Computer / Technology Usage
1. a) Recognizing why MSPs should prioritize service packaging and pricing to remain competitive. b) Identifying the components to build a service offering for exemplary service. c) Recalling five tools that simplify the work of MSPs through automation. d) Identifying specialized skills sought by MSPs for delivering excellent customer service. e) Identifying different responsibilities of an MSP to ensure daily functions and workflows. f) Understanding how service delivery functions contribute to the organization's success. g) Understanding why businesses implement technology solutions to scale, increase efficiency, and enhance cybersecurity awareness.	
Competency 3: The student will demonstrate the ability to provide excellent customer service by:	1. Communication 2. Critical thinking 3. Information Literacy 4. Computer / Technology Usage
1. a) Describing four strategies to deal with difficult customers positively. b) Recognizing the benefits of continuous product learning to meet evolving business needs. c) Understanding how to stay informed about industry trends to remain competitive. d) Defining the "Five Be’s" of effective communication to build trust with customers. e) Understanding how active listening combined with telephone skills can resolve issues. f) Applying three	

active listening techniques to telephone conversations to understand customer needs.	
Competency 4: The student will demonstrate proficiency in incident management and IT documentation by:	1. Communication 2. Numbers / Data 3. Critical thinking 4. Information Literacy 5. Computer / Technology Usage
1. a) Understanding how platforms such as Autotask and IT Glue support an MSP's Incident Management process. b) Recognizing the information detailed in a service request following a best practice framework such as ITIL. c) Listing examples of data managed in asset records to facilitate hardware troubleshooting. d) Understanding how processes can be documented in Autotask or IT Glue to drive standard operating procedures. e) Recalling key data required for time documentation to ensure accurate billing and reporting. f) Describing how expenses and charges are tracked against a ticket for efficient billing. g) Distinguishing between a service request and an incident to resolve support tickets efficiently.	
Competency 5: The student will demonstrate the ability to manage systems remotely by:	1. Communication 2. Critical thinking 3. Information Literacy 4. Computer / Technology Usage
1. a) Listing the functions of remote monitoring and management to assure IT operations stability. b) Listing four (4) benefits of RMM that reduce time spent resolving issues. c) Recalling the incident response features an RMM solution offers to address security threats. d) Recognizing how asset and inventory management	

enable firms to respond to changing business needs. e) Identifying the benefits of patch management to protect assets against cyber threats. f) Identifying key features of mobile device management (MDM) to protect mobile devices. g) Listing two (2) benefits of scripting that drive automation for repetitive processes. h) Identifying the key components of training to ensure full utilization of an RMM tool's capabilities	
Competency 6: The student will demonstrate the ability to ensure business continuity and recovery by:	1. Communication 2. Critical thinking 3. Information Literacy 4. Computer / Technology Usage
1. a) Identifying 3 types of backups that help ensure business continuity and data recovery. b) Identifying 3 rapid recovery technologies necessary to recover critical systems quickly. c) Successfully associating retention policies with various types of protected data. d) Identifying 5 security aspects of a backup appliance that may limit cyber-attacks. e) Increasing backup system efficiency by following backup scheduling best practices. f) Recognizing the importance of auditing backup strategy and solution health through regular reviews. g) Identifying common needs for practicing and verifying recovery plans and their importance and benefits.	
Competency 7: The student will demonstrate an understanding of security operations by:	1. Communication 2. Critical thinking 3. Information Literacy 4. Ethical Issues 5. Computer / Technology Usage
1. a) Describing three (3) examples of cyber-	

attacks that can exploit an organization's infrastructure. b) Recalling the main characteristics of three (3) common cyber threats that can compromise IT infrastructure. c) Listing the three (3) types of malware associated with cyber-attacks causing financial distress. d) Explaining the benefits of an Endpoint Detection and Response (EDR) platform to manage risks. e) Describing five (5) core components of an EDR platform to safeguard endpoints from advanced cyber-attacks. f) Listing the four (4) functions of a managed Security Operations Center (SOC) to safeguard against cyber threats. g) Explaining the benefits of a managed SOC to provide proactive defense against cyber threats. h) Understanding how comprehensive employee training can defend against phishing attacks. i) Describing how cybersecurity training & awareness software platforms such as BullPhish ID's phishing simulation can empower employees to respond to threats.	
Competency 8: The student will demonstrate proficiency in networking operations by:	1. Communication 2. Critical thinking 3. Information Literacy 4. Computer / Technology Usage
1. a) Defining key network protocol terminology and the OSI model to manage customers' data. b) Listing the steps to create a secure network to protect client data from malicious attacks. c) Describing three types of firewalls that protect a network from unauthorized access. d) Recalling different types of detection systems to detect, diagnose, and respond to potential security threats. e) Identifying encryption and access control protocols that mitigate security threats. f) Explaining how access control protocols can secure network communications and mitigate	

risks. g) Recalling two types of detection systems to detect, diagnose, and respond to potential threats.	

Updated: SPRING TERM 2024