Risk threat vulnerability essay

————————————————————- Week 2 Laboratory Perform a Qualitative Risk Assessment for an IT Infrastructure Learning Objectives and Outcomes Upon completing this lab, students will be able to: Define the purpose and objectives of an IT risk assessment * Align identified risks, threats, and vulnerabilities to an IT risk assessment that encompasses the seven domains of a typical IT infrastructure * Classify identified risks, threats, and vulnerabilities according to a qualitative risk assessment template * Prioritize classified risks, threats, and vulnerabilities according to the defined qualitative risk assessment scale * Craft an executive summary that addresses the risk assessment findings, risk assessment impact, and recommendations to remediate areas of non-compliance

Lab #4: Assessment Worksheet Perform a Qualitative Risk Assessment for an IT Infrastructure Overview The following risks, threats, and vulnerabilities were found in an IT infrastructure. Consider the scenario of a Healthcare provider under HIPPA compliance law and what compliance to HIPPA involves. 1. Given the list below, perform a qualitative risk assessment: Determine which typical IT domain is impacted by each risk/threat/vulnerability in the “ Primary Domain Impacted” column. Risk – Threat – VulnerabilityPrimary Domain ImpactedRisk Impact/Factor Unauthorized access from pubic InternetLAN – WANHigh

User destroys data in application and deletesLANHigh all files Hacker penetrates your IT infrastructure and gains access to your internal network System / ApplicationsHigh Intra-office employee romance gone badUser DomainLow Fire destroys primary data centerLan DomainHigh Service provider SLA is not achieved System / ApplicationsLow Workstation OS has a

known softwareLAN – WANMedium vulnerability Unauthorized access to organization owned User DomainHigh workstations Risk – Threat – VulnerabilityPrimary Domain ImpactedRisk Impact/Factor Loss of production dataLANHigh

Denial of service attack on organization DMZ and e-mail serverLAN – WANHigh Remote communications from home office LAN server OS has a known software vulnerability User downloads and clicks on an unknown unknown e-mail attachment Workstation browser has software vulnerability Mobile employee needs secure browser access to sales order entry system Service provider has a major network outage Weak ingress/egress traffic filtering degrades performance User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers VPN tunneling between remote computer nd ingress/egress router is needed WLAN access points are needed for LAN connectivity within a warehouse Need to prevent eavesdropping on WLAN due to customer privacy data access DoS/DDoS attack from the WAN/Internet 2. Next, for each of the identified risks, threats, and vulnerabilities, prioritize them by listing a “ 1”, “ 2”, and “ 3” next to each risk, threat, vulnerability in the “ Risk Impact/Factor” column. “ 1” = Critical, “ 2” = Major, “ 3” = Minor. Use the following qualitative risk impact/risk factor metrics: “ 1” Critical – a risk, threat, or vulnerability that impacts compliance (i. . , privacy law requirement for securing privacy data and implementing proper security controls, etc.) and places the organization in a position of increased liability “ 2” Major – a risk, threat, or vulnerability that impacts the C-I-A of an organization’s intellectual property assets and IT infrastructure “ 3” Minor – a

risk, threat, or vulnerability that can impact user or employee productivity or availability of the IT infrastructure 3. Craft an executive summary for management using the following 4-paragraph format.

The executive summary must address the following topics: * Purpose of the risk assessment & summary of risks, threats, and vulnerabilities found throughout the IT infrastructure * Prioritization of critical, major, minor risk assessment elements * Risk assessment and risk impact summary * Recommendations and next steps Week 2 Lab: Assessment Worksheet Perform a Qualitative Risk Assessment for an IT Infrastructure Overview Answer the following Assessment Worksheet questions pertaining to your qualitative IT risk assessment you performed. Lab Assessment Questions & Answers . What is the goal or objective of an IT risk assessment? 2. Why is it difficult to conduct a qualitative risk assessment for an IT infrastructure? 3. What was your rationale in assigning “ 1” risk impact/ risk factor value of “ Critical” for an identified risk, threat, or vulnerability? 4. When you assembled all of the “ 1” and “ 2” and “ 3” risk impact/risk factor values to the identified risks, threats, and vulnerabilities, how did you prioritize the “ 1”, “ 2”, and “ 3” risk elements? What would you say to executive management in regards to your final recommended prioritization?