Northeastern University
Khoury College of
Computer Sciences

Master of Science in Cybesecurity

Northeastern is designated by NSA and DHS as a Center of Academic Excellence in Cyber Defense, Research, and Cyber Operations

Security Risk Management and Assessment

Course Number: CY 5200
Total Credit Hours: 4
Instructor: Themis A. Papageorge, Associate Clinical Professor, Director of Information Assurance and Cyber Security Employer Relations

Create an MS-Word document which should describe your Risk Management Plan for HGA. The document should be organized as described below:

I. Title page

II. Table of contents

III. Executive summary based on the data of the NIST template points 1-15 (one or two pages) discussed in Class 4. You can make assumptions if the HGA case does not provide the required data, e.g. for Information System Security Plan Approval Date you can use the Due Date for Assignment 4. Then you can include your work from Assignments 1-3. You need to use the MOT 17 risk control "families" in Point 13. Detailed spreadsheet tables can be included in the following sections of your paper or in the Appendix.

IV. List of Assets with Values ($)

V. List of Threats

VI. List of Vulnerabilities

VII. Threat/Vulnerability pairs (with probabilities 0%-100% that a threat will exploit the specific vulnerability)

VIII. Assets impacted by Threat/Vulnerability pairs

IX. MOT – which MOT controls are covered by current HGA controls (Histogram)

X. MOT – which MOT controls are covered by current AND proposed by new CISO HGA controls AND VPN server AND DMZ (Histogram)

XI. Security Risk Prevention Strategy: Security Risk ($) Calculations of Assets with vulnerabilities discovered by new CISO and protected by current controls. Calculate residual risks for assets and total HGA residual risk. Calculate vulnerability risks for ranking which vulnerability should be addressed by controls first, second, third etc.

XII. Security Risk Prevention Strategy: Security Risk ($) Calculations of Assets with vulnerabilities discovered by new CISO and protected by current and proposed by new CISO controls. Calculate residual risks for assets and total HGA residual risk. Calculate vulnerability risks for ranking of which vulnerability should be addressed by controls first, second, third etc.

XIII. Security Risk Prevention Strategy: Security Risk ($) Calculations of Assets with vulnerabilities discovered by new CISO and protected by current and proposed by new CISO controls and non-covered/missing MOT controls. Calculate residual risks for assets and total HGA residual risk. Calculate vulnerability risks for ranking which vulnerability should be addressed by controls first, second, third etc. Compare HGA current, CISO proposed, and VPN and DMZ risk controls to the 157 risk controls from Common Criteria.

XIV. Security Risk Prevention Strategy and Security Risk Response (Resilience) Strategy: Apply Hardening Controls to highest ranked Residual Asset Risk, thus reducing Risk Impact probabilities, and further reducing the overall security asset residual risk. Calculate residual risks for assets and total HGA residual risk. Provide a ranking for which vulnerability should be addressed by controls first, second, third etc. and a ranking for which risk impact should be addressed by controls first, second, third etc. Compare HGA current, CISO proposed, and VPN and DMZ risk controls to the 157 risk controls from Common Criteria.

Calculate for a Security Risk Prevention Strategy, and a Security Risk Response (Resilience) Strategy, and a Mixed (combination of the two) Strategy residual risks for assets and total HGA residual risk, vulnerability risks for ranking which vulnerability should be addressed by controls first, second, third etc. and a ranking for which risk impact should be addressed by controls first, second, third etc. for the 3 Security Strategies (Prevention, Response, Mixed).

XV. Conclusion: Cost Benefit Analysis. Did the HGA team address all security risks based on your risk assessment for HGA? What would the budget for proposed controls be including controls proposed by new CISO controls and missing MOT controls and VPN and DMZ? Do you recommend a Risk Prevention Strategy or a Risk Response Strategy or a combination of both? Does the residual risk reduction exceed the budget for proposed controls? What is the ((proposed security risk budget Cost) / (expected security risk Benefit)) ratio?