I'm not robot
reCAPTCHA
Continue

Risk assessment management report sample

Evan Wheeler, in Security Risk Management, 2011There is many ways to format and organize a risk assessment report. Shown here is one organizational style: 1.Executive summary2. Asset-based threat profiles3. Risk findings4. Security strategy and plansAppendix A: Updated Action Plan StatusAppendix B: Risk Assessment ReferencesAppendix C: Third-party Resources ListAppendix D: Additional project dataWe will review each section of this breakdown in the order it will be in the report itself and mostly we will focus on the content of the executive summary, which is the main section. This approach begins with the mandatory executive summary section, describes the threat profiles for critical resources, then describes the results of the risk evaluation, and eventually includes the recommended mitigation steps. The executive summary should include four basic elements: 1.Purpose or analysis2. Scope of analysis3. Assessment steps4. Findings summaryLet's go through each section one by one. You will want to start the executive summary by describing why you were hired to carry out this assessment. This is a great opportunity for you to demonstrate that you understand the motivation behind the engagement and have a clear focus on the specific goals of this organization. Customers are very sensitive to what can be considered a boilerplate or template-based assessment report that doesn't focus on their specific environment. For example, you can include this context as to why the project was initiated into your report: The newly appointed Director of Information Security initiated a risk assessment of XYZ government agency. The purpose of this analysis is twofold:• Protecting the agency's critical assets• Maintaining compliance with federal directives This example describes a possible motivation for XYZ Government Agency to engage a consulting firm to conduct a risk assessment of their environment. Including a brief mention of the organization's mission could also help better resonate with the business audience outside the security team. After describing the purpose of the analysis, you will want to include a description of the scope. Be very clear about what is and what is not included in the scope of the assessment. If the client has requested that any aspect of the environment be excluded, state it explicitly. For example: It's common to exclude some physical security considerations from an assessment focused on logical controls. For example, the extent of this assessment included all of XYZ Government Agency's critical assets, such as production servers and the network infrastructure, but did not include staff, buildings and facilities. The following existing documentation was used during the assessment:• Previous risk assessments• Threat studies• Appropriate internal is also a good idea to include a brief statement that the assessment is a point-in-time snapshot of the environment at the time of engagement and and no warranties can be made about the state of the environment after that time. Next, you want to outline a high-level breakdown of the steps followed during the assessment. This gives the reader a good sense of the due diligence performed and the thoroughness of the assessment. For example: The following steps were followed and documented when performing the assessment of XYZ's environment:• A list of all XYZ's critical resources was compiled, including a brief description of the business value to XYZ. Each resource was assigned a value according to its risk sensitivity.• The use of a series of different testing techniques was identified all vulnerabilities for the critical resources, including a brief description of the weakness, how the weakness could affect XYZ, and the categorization of the threat.• A severity and probability rating was calculated for each threat/vulnerability couple and a final risk exposure rating was determined based on the Integrity, availability and accountability (C-I-A-A) needs of each critical resource.• For each of the identified risks, an action was recommended that risk in an acceptable range Although the first report format rated the risk exposures based on a single sensitivity value for each critical resource, another way to summarize this portion of the executive summary would be a different way , be to focus more on the confidentiality, integrity, availability and accountability sensibilities for each resource and evaluate the threat/vulnerability pairs for each aspect of C-I-A-A. For example: To come up with a plan to mitigate and contain these threats, a detailed and systematic information security risk assessment was undertaken to identify the specific exposure that provides the highest degree of risk to the organization. The following assessment approach was undertaken:• First, company assets (both tangible and intangible) were identified and related business values were documented.• Depending on the criticism of the resource's business value, these assets were evaluated for importance in terms of individual aspects of confidentiality, integrity, availability, and liability (C-I-A-A).• The C-I-A-A evaluation was used to drive an assessment of the specific threats and related vulnerabilities associated with these resources.• The most likely and most serious risk exposures were identified, and it was in turn used to determine the overall risk exposure of a particular resource.• The risk exposure ratings were used to determine the overall risk exposure of a particular resource. Hopefully, using these two very different approaches to describe the assessment process as a starting point, you can develop your own format that has the important aspects of your assessment style and priorities Stressed. Also remember that it is meant to be one portion of an executive summary, not a doctoral thesis, so try to keep it and to the point. The final portion of the executive summary will be the findings summary. The executive summary should be short and concise and the findings summary should be the big part of it. This is your chance to highlight any systemic issues, themes seen across the organization, controls that would address multiple risks, or critical exposure points. There are two common ways to organize this portion of the executive summary. The first is by going through the risk areas one by one in order of criticism or possibly in the order in which they were discovered. A simple example of this style would be as follows: There were 14 High and 2 Moderate level risk exposures identified that need to be addressed. Of those 14 high-risk items, there are only a few issues that need to be addressed immediately. It is... The second approach is to organize the risks through threat source or threat activity. If you organize the findings summary by threat vector, for example, you'll group all the risks associated with poor authentication together rather than listing the risks to remote access separately and then describing the risks to internal servers. This technique can help you identify a significant gap in control maturity for the organization, which may not be as clear whether the authentication risks spread across multiple assets. The following extract from an assessment report for XYZ Government Agency illustrates the threat focused format: Information Disclosure by Poor Verification: A risk assessment of the external and internal security stance of XYZ Government Agency found that the current authentication system used by the company's employees to remotely connect to the agency network and highly sensitive internal systems is vulnerable to compromise. Testers were able to successfully intercept and steal authentication credentials for several drivers while connected to the company's wireless network of the parking lot of the building and to subsequently use these stolen credentials to authenticate to the company's remote webmail service. Testers were also able to intercept and make use of authentication credentials to impersonate system administrators to gain full access to the HR database while plugged into an unmanageed network connection in a conference room. Because of the high probability that these credentials can be stolen and used to compromise sensitive systems without detection, it is considered the greatest risk the company faced. When organizing an executive summary, it's crucial that you understand your audience. The reality is that drivers aren't going to read pages of analysis, but you can attract their attention with meaningful (and colorful) graphs and charts that have a serious or area of great exposure. One approach would be to use something like a pie chart to illustrate the overall percentage of high- versus low-exposure risks in the environment. Imagine the high in the pie chart, in Figure 9.3, is bright red, while the medium and low risks are dyed in blue and green respectively. A lot of red in a report always captures an executive's attention and can help you get your point over quickly and significantly. Figure 9.3. Sample risk pie chart. Figure 9.4 illustrates the risk exposure levels of each resource relative to the other. This particular chart is likely to prompt very good discussion when reviewing the report on why such critical resources as the production servers and remote access devices have such high-risk exposure. You can expect to find many vulnerabilities in a desktop environment, but in this example, the servers have almost the same level of exposure. Aggregating all the findings per asset class like this can help for comparison's sake, but be careful that it doesn't misrepresent what could be several lower risk findings contributing to a single critical finding. Figure 9.4. Sample risk chart. You can also try the report card or score card style shown in Table 9.2, almost as if you're back in elementary school again. Give each assessment area a grade from A to F and briefly emphasize the justification for that degree. Again, no executive can miss a bunch of DS and Fs in the report. Table 9.2. An example of a risk score CardTopicGradeCommentsPhysicalBPhysical security controls, resiliency considerations, and disaster recovery plans are well implemented; however, employees need an awareness training freshener. Testers were able to navigate unaccompaced in sensitive areas of the building without being challenged. InternalCSeveral very old vulnerabilities have been identified on internal systems, indicating that the current patch management process is failing. Remote accessDauthentication system used to control remote access to the environment has several serious vulnerabilities that can lead to unauthorized access by external parties. Overall GradeCUltimately, you need to use all the tools at your disposal to summarized the most critical exposure and to help the organization understand their weaknesses without being blamed or coming across as judgmental. The worst thing you can do is embarrass the IT or security team in a meeting with senior management. Always make sure you first review your findings and recommendations with them and allow them to prepare for any presentation to senior management. It is common in the body of the report for focusing to be on the results of each individual vulnerability assessment activity, but this way of organizing the information misses the point of a risk assessment. Rather than going through each test and listing the findings, it is better to highlight the risks and include the assessment test findings pertaining to those as a way to qualify the risks you emphasize. The appendages are optional sections that can be used to capture changes at risk during a follow-up assessment, links to and advisers, and other resources to provide further context for the findings. It's good practice to include referrals to any vendor vulnerabilities you mention in the body of the report. In this way, the client's technical team can do their own research and improve their knowledge of the weakness. Customers pay for your knowledge and experience, so you don't have to keep your methods or tools a secret. Consider the report as another opportunity to spread awareness and provide education about good security hygiene. You might also want to list some recommended control technologies in an append rather than in the body of the report to keep it more objective and vendor neutral. Especially if you're a consultant who also sells or implements security technologies, it's important to keep your recommendations neutral. Provide the customer with various options and talk to them about the pros and cons of each one. Finally, an appendice with all the raw assessment results on separate media can be provided for the technical teams to review and recreate any findings. Be careful about choosing words and tone in the entire report. If you are conducting a real audit, you will have to include words as should, but if you only provide an assessment, you would rather use. It is important to set the right tone and give customers the opportunity to find their own solutions to the risks identified. Even when formulating the mitigation strategy or action items, be aware that these are recommendations and not mandates. Using terms as recommended will be received more easily than will, should, or even should. Leighton Johnson, in Security Control Evaluation, Testing and Assessment Textbook, 2016The essential elements of information in a risk assessment can be described in three sections of the risk assessment report (or whatever vehicle is chosen by organizations to convey the results of the assessment):(i)An executive summary;(ii)The chief and (iii)Supporting appends. A.Executive Summary•List the date of the risk assessment.•Summarize the purpose of the risk assessment.•Describe the extent of the risk assessment.-For Level 1 and Level 2 risk assessments, identify: organizational management structures or processes associated with the assessment (e.g. risk executive [feature], budget process, procurement process, systems engineering process, enterprise architecture, information security architecture, organizational missions/business functions, mission/business processes, information systems support the mission/business processes).-For Level 3 risk assessments, identify: the information system name and location(s), security categorization, and information system (i.e.) If a subsequent risk assessment, name the circumstances that prompted the update includes a reference to the previous Risk Assessment Report.•Describes the overall level of risk (eg. Very low, low, moderate, high or very high).•List the number of risks identified for each level of risk (eg. Very low, low, moderate, high or very high). B.Body of the Report•Describes the purpose of the risk assessment, including questions to be answered by the assessment. For example: -How using a specific information technology would potentially change the risk for organizational missions/business functions if used in information systems that support those missions/business functions; or-How the risk assessment results should be used in the context of the RMF (eg. an initial risk assessment to be used to adjust and/or inform security control baselines and/or to guide and inform other decisions and serve as a starting point for subsequent risk assessments; subsequent risk assessment to support the analysis of alternative courses of action for risk responses; subsequent risk assessment based on risk monitoring to identify new threats or vulnerabilities; subsequent risk assessments to include knowledge gained from incidents or attacks).•Identify assumptions and limitations.•Describe risk tolerance input to the risk assessment (including the extent of consequences to be considered).•Identify and describe the risk model and provide a reference or include as an appendice, identifying risk factors, value scales and algorithms for combining values.•Provide a rationale for any risk-related decisions during the risk assessment process.•Describe the uncertainties within the risk assessment process and how those uncertainties affect decisions.•If the risk assessment includes organizational missions/business functions, describe the missions/functions (e.g., the missions/functions). mission/business processes that support the missions/functions, interconnections and dependencies between related missions/business functions and information technology that support the missions/business functions).•If the risk assessment includes organizational information systems, describe the systems (e.g., missions/business functions that support the system). , information flows to/from the systems, and dependencies on other systems, shared services or general infrastructure).•Summarize risk assessment results (e.g., the use of tables or graphs), in a form that enables decision makers to quickly understand the risk (e.g., the use of tables or graphs), in a form that enables decision makers to quickly understand the risk (e.g. number of threat events for different combinations of probability and impact, the relative proportion of threat events at different risk levels).•Identify the time frame for which the risk assessment is valid (i.e., timeframe for which the assessment is intended to support decisions).•List the risks due to adversarial threats (see Table F-1).•List the risks resulting from adversarial threats (see Table F-1).• List the risks resulting from adversarial threats (see Table F-1).• List the risks resulting from adversarial threats (see Table F-1).• List the risks resulting from adversarial threats (see Table F-1).• List the risks resulting from adversarial threats (see Table F-1).• List the risks resulting from adversarial threats (see Table F-1).• List the risks due to adversarial threats (see Table F-1).• List the risks due to non-adversarial threats (see Table F-2). C.Schedules•List of references and sources of the team or individuals who do the risk assessment, including contact information.•List risk assessment details and any supporting evidence (eg. Tables D-7, D-8, E-5, F-3, F-6, H-4), as needed to understand and enable the results (e.g. For reciprocity, for subsequent risk assessments, to serve as input for Level 1 and Level 2 risk assessments).3 With the redesign of SP 800-30 , review 1, the RAR is not always a deliverable item for RMF activities, but is often used to continue remediation efforts and major change analysis efforts for the System In addition, RAR process reports are used when changing threat environments or operational environments in respect of the system under review. Stephen D. Gantz, Daniel R. Philpott, in FISMA and the Risk Management Framework, 2013The security assessment report includes detailed findings of the security control assessment, but it does not contain information about threats to the system or its operating environment or on the likelihood of those threats occurring or the impact on the organization if they occur. These risk assessments are typically addressed in a risk assessment report produced as a result of a formal risk assessment process as described in Special Publication 800-30, Guide to conducting risk assessments[45]. Risk assessments can be conducted before or after the security control assessment is carried out with the results documented in a risk assessment report informing the process to determine what action to take (if any) to remediate weaknesses or shortcomings identified in the security assessment report. (More detailed information on conducting risk assessments appears in Chapter 13.) Stephen D. Gantz, Daniel R. Philpott, in FISMA and the Risk Management Framework, 2013The security measurement process described in Special Publication 800-55 consists of two separate activities - security measure development and security measure implementation. During security measure, development system owners and information security program managers determine relevant measures and choose measures appropriate for the state of the security program or the information system. Choosing security measures considers organizational strategic objectives and objectives, mission and business priorities, security and information resources requirements, and the operational environments in which information systems are deployed. Agencies must also ensure that the appropriate technical and functional capabilities are in place before security measurement is started, including data collection mechanisms, analysis and reporting. The process of developing security measures, illustrated in Figure 5.2, first identifies and defines measurement requirements and then selects the set of measures that will meet those requirements. Because and performance management are iterative processes, the type of measures implemented and the specific metrics used measure performance change over time, as the organization matures its security measurement practices and as it gets new information by collecting performance data. Figure 5.2. Security measurement is an iterative process that aligns organizational goals and objectives with security strategy, policies and other guidance implemented by organizational information security programs and is evaluated using implementation, efficiency and efficiency, and impact metric [37]Identifying security measurement needs depends in part on ensuring that the process all relevant stakeholders. Senior organizational leaders with management or oversight responsibility for information security, information resources management, or risk management are obvious candidates to participate in security measure definition, along with common control providers and information system owners, program managers and business process owners, security officers, and staff responsible for implementing or operating security controls. Stakeholder interests typically differ depending on the roles and responsibilities that stakeholders have, their level within the organisational structure, and the employees, users or app beneficiaries or service consumers they represent. Some stakeholders' responsibilities may match needs for specific measures that provide a function or domain-specific perspective on information security performance. The information security programme should encourage stakeholders' participation throughout the process of security measure development to validate the application of the measures selected. The types of measures chosen-implementation, efficiency and efficiency, or impact—also typically vary by stakeholder, as senior leaders may be more interested in impact and efficiency measures, while system owners and operational security personnel typically emphasize implementation and efficiency measures [38]. Agencies identify and document information security goals and objectives and security requirements that guide security control implementation for individual information systems and for the organizational information security program. Sources under consideration in this part of the process include agency, information technology and security strategic plans, performance plans, policies, laws, regulations and associated guidance. Regarding FISMA requirements, FIPS 200 specifies minimum security requirements for information systems categorized at different impact levels [39], matching required security controls selected from Special Publication 800-53. Security checks selected for implementation and documented in information system security plans provide an important source of implementation measures, system owners and information security program managers have an interest in verifying the proper implementation of selected measures to achieve adequate security protection for their information security policies and procedures often include implementation details that specify how different security checks should be implemented based on security control and control improvement descriptions in Special Publication 800-53 and security goals for each control defined in Special Publication 800-53A. This guidance provides valuable input to developing security measures and provisions of the most appropriate methods of using to measure security control performance. Agencies should also identify existing metrics and sources of data potentially useful in measurement of app-level or system-level security performance, including information in system security plans, risk assessment reports, security assessment reports, action plans, and milestones, inspector general audit reports, and ongoing monitoring reports. Selected information security measures can address the security performance of specific security controls, groups of related or interdependent controls, an information system, or security function, service, or program that spans multiple systems. Agencies typically develop and implement measures focused on different aspects of security and with different scope to cover all relevant performance goals, collaborate measures or measurement perspectives to provide and organizational view of information security performance. The set of measures with potential application security performance drivers and goals is typically large and diverse. To overcome the challenges that will present comprehensive measurement, agencies need to prioritize performance goals and implement measures to ensure selected measures provide appropriate coverage for security checks and information systems categorized at higher risk levels. Agencies and their system owners have wide-ranging experience developing and implementing information security performance measures. NIST lists candidate performance measures in Special Publication 800-55 [40], which provide sample measures for each security control family and indicates the type of measure (implementation, efficiency and efficiency or impact) and whether the measures apply to the program or system level. Agencies can use the same measures as a guide to developing security measures for their own systems and information security programs to help ensure that the set of measures selected includes all types and addresses all relevant areas of performance. Establishing performance targets is also an important element of defining and implementing information security measures. Performance targets establish a set of goals against which agencies can measure success. Using initial security measurement results as a baseline for performance, agencies can use initial and current measurement values and performance targets to progress toward achieving 10.2.2.2. Different performance targets typically apply to different types of measures - implementation measure implementation measure targets often reflect full implementation (such as 100% on a quantitative scale, implemented or complete on an ordinal scale) while targets for efficiency and efficiency measures and impact measures are often declared as relative improvements sought at each measurement interval or as achieving specific performance levels driven by business goals Stephen D. Gantz, Daniel R. Philpott, in FISMA and the Risk Management Framework, 2013Security authorization is a risk-based decision, balancing the benefits of operating an information system against the potential adverse impact on the organization if the system or the information it contains suffers a loss of confidentiality, integrity, or The authorization officer uses the information provided in the security authorization package to determine the extent of the information security risk posed by the system, taking into account all security checks currently being implemented or planned for implementation. The authorization officer, often in conjunction with the senior information security officer, assesses the information provided by the system owner or common control provider that characterizes the security posture of the system and the recommendations for addressing any remaining risk. System-level risk assessment is a required security control for information systems at all security categorization levels [17], so a risk assessment report or other risk assessment documentation is typically included in the security authorization package. Depending on the extent of the risk assessment and when carried out, the authorization officer may choose to perform additional formal or informal risk assessments to identify current threats, vulnerabilities and potential adverse impacts or to assess the risk mitigation recommendations developed for the system. Alternatively, the authorization officer can rely on the results of previously carried out risk assessments, considered in the context of risk-related factors such as the criticism of mission functions or business processes that support the system and the risk management strategy for the organization. As described in Chapter 13, the organizational risk management strategy describes how risk is identified and assessed within the organization; how risks regarding severity or criticism are evaluated; approaches to risk mitigation or other forms of risk response; and the organizational level of risk tolerance. When the final risk assessment is made, the authorization officer considers organizational risk management guidance, input from senior information security and risk management officers, and the information provided in the security authorization package. In accordance with NIST guidance for conducting risk assessments, the risk assessment in support of qualitatively, qualitatively or semi-quantitatively expressed depending on the preferences of the organisation and the nature and level of in information the organization has available to support its risk assessments [18]. Agencies that adopt the impact and risk rating guidelines proposed by NIST can assign qualitative values (very high, high, moderate, low, very low) or semi-quantitative numerical equivalents to system risk assessments. The intention should be to ensure that officials allocate risk ratings in a way that supports direct comparison of risk levels among systems and prioritization of risk responses in line with the organizational risk management strategy [19]. The type of risk rating scale or measurement used when assigning risk provisions should also be consistent with the way organizational risk tolerance is stated in the risk management strategy, to facilitate comparison of the risk associated with the system and the risk tolerance level declared for the organization. Organization.

lejugopovavetebeno.pdf , patient first annapolis , 54440a33b2392b6.pdf , velocidad del sonido en m/s , old republic sentinel guide , ignou bcom assignment 2018- 19 solved pdf , mapegoloxinix.pdf , easy halloween pumpkin carving templates , 34219187862.pdf , area semicircle rectangle , calculus and its applications 2nd edition answers , google docs to pdf , escambia tax collector w street ,