SafeAssign Originality Report

Fall 2020 - Enterprise Risk Management (ITS-835-M52) - Full Term • Week 8 Research Paper

View Originality Report - Old Design

Sai Balaji Yamsani

Submission UUID: 7b14e283-9f2e-d958-984e-c5854e6984d6

Total Score: High risk 71 %

Total Number of Reports	Highest Match	Average Match	Submitted on	Average Word Count
1	71 % week8.docx	71 %	12/04/20 08:54 PM EST	1,555 Highest: week8.docx

Attachment 1 71 %

Word Count: 1,555
week8.docx

Institutional database (9) 68 %

(1) Student paper
(3) Student paper
(4) Student paper
(6) Student paper
(8) Student paper
(2) Student paper
(7) Student paper
(5) Student paper
(11) Student paper

Global database (1) 2 %

(9) Student paper

Internet (1) 1 %

(10) scpslab

Top sources (3)

(1) Student paper
(3) Student paper
(4) Student paper

Excluded sources (0)

(1) Enterprise Risk Management 1

Enterprise Risk Management 2

Sai Balaji Yamsani

(2) University of the Cumberland's

Introduction

Baseline controls are known for helping institutions in minimizing the data breaches and cyber security occurrences risk. They have their focus on having the risk reduced and the way the organization get to respond to the occurrences. It is recommendable that institution is to adopt the idea of them suffering from breach of data during their operations hence the need of being prepared in detecting, responding as well as recovering. (3) These are the possible requirements for baseline security applicable into the implementation as well as design during usage of cloud computing within the framework of enterprise risk management. (1) Applications baseline security include: Understanding the firm's background – application risk minimization occurs within the sense of an organization. (1) Basically, risks are considered to be inevitable in addition to be essential during applications development. Management of risk inclusive of the risk avoidance concepts as well as trade-off of techniques, tends to have an influence that is of significance on the performance of a business. Identification of the technological as well as enterprise risks that might involved – this is because the enterprise risks tend to impact the consumer business objectives. (3) Having the threats identified is crucial in explaining as well as measuring the available possibility that these occurrences might have an effect that is direct on the objectives of the enterprise. (4) The risks of an enterprise comprise of impacts that tend to include reputation or product harm, regulatory or consumer requirements violation, increased expenses for development, vulnerability to liability in addition to financial loss that is direct. (1) Extraction as well as prioritization of risks, in addition to generating a collection

that is ranked, there tends to be a number that is significant of risks within almost each specific procedure. To identify these risk levels is of great importance, however, having such risks prioritized is crucial in resulting into success of a business. It is evident that the process of prioritization is supposed to consider the objectives of the business that are considered to be most critical to the organization, there is direct threatening of goals as well as the possibility of the technological complexities get expressed in a manner that it tends to impact the organization. (1) There is definition of the risk reduction technology whereby putting into consideration the risk collection as well as their objectives from the third phase, there is establishment of a coherent strategy of risk reduction in a manner that is cost-effective. Any activities for mitigation that have been proposed are supposed to factor in costa, implementation time, accuracy, success opportunities as well as the general impact over the complete datasets of risk. Having the issues fixed as well as having the fix validated which is a phase that involves usage of the techniques for validation that have been identified recently. (1) Validation phase provides some surety that there is adequate mitigation of risks via development of item in addition to the approach of risk reduction being effective.(Fagan, et.al, 2020). Databases baseline security

Classification which involves preparation through taking general business data overview within the system of the user, if it is present within a document of Windows on a given drive that is said to be local within a Microsoft office based within cloud. Then identification of information that is sensitive which can be accessed by individuals who are not authorized in addition to data that is stack at the absence of any business value that is immediate. Selection which occurs after definition of crucial data by the users, hence the essence of choosing controls that are suitable for the FIPS 200 program and standard publication 800-53 of NIST. Implementation Involves creation or modification of an event response ability through having employees trained on regular management, keeping track of events, permissions for users as well as management of directory. After knowing the destination of the information that is most crucial, there is essence of monitoring the ones having exposure to it. (3) Assessing involves preparation for responding through evaluation of probable risks of safety in addition to mitigation prioritization. (1) Automation ensures maintenance of the Security framework of the agency, as well as having the given violations rectified and preservation of the model that is least privileged. Additionally, continue monitoring and having data quarantined and making sure that essential as well as state data get to be managed appropriately by the given governments (HaddadPajouh, et.al, 2019). Authorization involves implementation of a data workflow as well as regulation that is agreed upon, being ready to have the rule enforced by having the variances on addition to returning to state that is reliable.

(1) Additionally, there is making sure that any data capable of being impacted as an event's part gets safeguarded through archiving, deleting in addition to archiving or having them migrated into places that are different. Monitoring whereby with the data security being on site, users are supposed to maintain as well as have constant improvement. (3) There is monitoring of the policies of security through automation and making sure that the organizations' cyber hygiene is safeguarded and also monitored. (5) System's baseline Security Requirements include: (1) Categorizing the systems of information whereby it is a phase that is administrative and understanding the organizations' awareness. Boundary of the system needs establishment prior to identification of the system. Through system boundary, general form of information regarding the system should be identified. (3) Selection of management of security that indicates the controls for security are operational, technological in addition to administrative controls and techniques of prevention that are utilized within information system of the company, accountable for preserving security, the availability in addition to the systems integrity and information. (1) Implementation of management of security whereby the third phase needs a firm to carry out controls of security and identification on the manner in which the control systems get utilized in the system of data in addition to operating setting. Assessing the system of security control includes utilization of evaluation formula that is suitable in establishing the severity of proper implementation of the controls on order to function on the most suitable means so as the again the requirements of safety for the given system. Authorization of the system of information that aims on risk assessment to the firm's persons and processes, among others rising from the data system application and an assessment of the risk being suitable (Ghani, et.al, 2019). (1) Monitoring management of security enables the organization in retaining the clearance security of a system of data for a long duration within an operating setting that is changing rapidly where the systems make adjustments to vulnerabilities, threats, technology that are evolving and the processes of a business. Network Infrastructure baseline security include: Categorizing the system or framework in addition to the data that it gathers, keeps and transmits depending on the effective analysis. Selection involves a prior gathering of security controls that are basic belonging to the systems depending on the categorization of the security. (1) Implementation of the measures of security and recording the manner in which the controls get implemented within the system as well as the operating surrounding. (6) Assessing the controls to utilize procedures that are appropriate in describing the validity which the systems of control are implemented appropriately. (1) Authorization whereby the operation program ends up focusing on the risk evaluation to the effectiveness of the organization and assets, individuals among other agencies and nation. (3) Monitoring and evaluation of system security policies that are chosen on a process that is continuous. (7) Information processing baseline

(3) The framework for management of risk provides a structured, organized and plan that is responsible in identifying privacy and security risks, inclusive of the classification of information security. (1) In addition, the framework also encourages strategic planning that is near-real-time and information system that is ongoing and control authorization via monitoring procedures that are continuous, offers the executives and senior managers with needed data for making decisions for managing risk that are efficient and cost effective. (Kumar and Goyal, 2019). (1) The Risk management framework implementation connects crucial RMF at the risk management performance at the network level at the institution level. (8) Additionally, it offers transparency and accountability for performed controls through organizations' information systems. Conclusion

The baseline controls have an objective of advising as well as guiding institutions on the manner in which they ought to maximize the cyber security investments effectiveness and efficiency. The organizations that are making attempts of going beyond the controls, they are required to invest into cyber security measures that are more comprehensive like Center for the Internet Security Controls.

References: (3) Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020). (3) IoT Device Cybersecurity Capability Core Baseline (No. NIST Internal or Interagency Report (NISTIR) 8259A). National Institute of Standards and Technology. Ghani, A., Mansoor, K., Mehmood, S., Chaudhry, S. A., Rahman, A. U., & Najmus Saqib, M. (2019). (9) Security and key management in IoT-based wireless sensor networks: An authentication protocol using symmetric key. International Journal of Communication Systems, 32(16), e4139. HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H.

(2019). (10) A survey on internet of things security: Requirements, challenges, and solutions. (11) Internet of Things, 100129. (2) Kumar, R., & Goyal, R. (2019). (3) On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. (3) Computer Science Review, 33, 1-48.

Source Matches (37)

1 Student paper 81%

Student paper

Enterprise Risk Management 1 Enterprise Risk Management 2

Original source

Enterprise Risk Management Enterprise Risk Management

2 Student paper 100%

Student paper

University of the Cumberland's

Original source

University of the Cumberland's

3 Student paper 73%

Student paper

These are the possible requirements for baseline security applicable into the implementation as well as design during usage of cloud computing within the framework of enterprise risk management.

Original source

These are the baselines requirements for security capable of being applied into the design as well as implementation during use of cloud computing in risk management of an enterprise

1 Student paper 83%

Student paper

Applications baseline security include:

Original source

Baseline security of applications

1 Student paper 74%

Student paper

Basically, risks are considered to be inevitable in addition to be essential during applications development. Management of risk inclusive of the risk avoidance concepts as well as trade-off of techniques, tends to have an influence that is of significance on the performance of a business. Identification of the technological as well as enterprise risks that might involved – this is because the enterprise risks tend to impact the consumer business objectives.

Original source

Risks tend to be inevitable in addition to being an essential part during the applications development The management of risk, inclusive of concepts in relation to the avoidance of risk as well as trade-off that is technological are considered to have an influence that is of great significance on the performance of a business Identification of the technological as well as the enterprise risks that are involved- the risks of a business are considered to have one or more impacts on the business objectives in relation to the consumer

3 Student paper 66%

Student paper

Having the threats identified is crucial in explaining as well as measuring the available possibility that these occurrences might have an effect that is direct on the objectives of the enterprise.

Original source

Identification of the threats help in explaining and measuring the possibility that these events might have an effect which is direct on the objectives of a business

4 Student paper 79%

Student paper

The risks of an enterprise comprise of impacts that tend to include reputation or product harm, regulatory or consumer requirements violation, increased expenses for development, vulnerability to liability in addition to financial loss that is direct.

Original source

Business risks involve impacts that also include direct financial loss, harm to product or reputation, violation of consumer or regulatory requirements, vulnerability to liability, and increased development costs

Student paper 65%

Student paper

Extraction as well as prioritization of risks, in addition to generating a collection that is ranked, there tends to be a number that is significant of risks within almost each specific procedure. To identify these risk levels is of great importance, however, having such risks prioritized is crucial in resulting into success of a business.

Original source

Extracting in addition to having the risks prioritized, as well as generation of a collection that is ranked – this is considered to be essential mainly because there is the availability of a number that is significant regarding risks within almost each given process Identification of the risk levels is of great importance, however, giving priority to the various risks is what results into the success of a business

Student paper 70%

Student paper

There is definition of the risk reduction technology whereby putting into consideration the risk collection as well as their objectives from the third phase, there is establishment of a coherent strategy of risk reduction in a manner that is cost-effective. Any activities for mitigation that have been proposed are supposed to factor in costa, implementation time, accuracy, success opportunities as well as the general impact over the complete datasets of risk.

Original source

Another requirement is defining the risk reduction technique – this includes putting into consideration the gathering of risks in addition to their objectives from the third phase, the following step involves establishment of a coherent strategy on the reduction of risk on a manner that is cost effective Any activities that are proposed on mitigation, are supposed to factor in implementation time, expenses, success opportunities, effectiveness as well as impact over the overall datasets of risk (Pérez-Cornejo, et.al, 2019)

Student paper 75%

Student paper

Validation phase provides some surety that there is adequate mitigation of risks via development of item in addition to the approach of risk reduction being effective.(Fagan, et.al, 2020). Databases baseline security Classification which involves preparation through taking general business data overview within the system of the user, if it is present within a document of Windows on a given drive that is said to be local within a Microsoft office based within cloud. Then identification of information that is sensitive which can be accessed by individuals who are not authorized in addition to data that is stack at the absence of any business value that is immediate.

Original source

The validation phase provides some sort of assurance that the risks have undergone adequate mitigation by development of item in addition to the approach of risk reduction being operational Baseline security of databases Categorization that includes preparing through having an overview of general data of the business the system of the user, if its existence is within a document of Windows on a drive that is local or within a Microsoft office cloud Identify information that is sensitive and accessible to individuals that are not authorized in addition to having data stacked that has no business value that is immediate

Student paper 63%

Student paper

Selection which occurs after definition of crucial data by the users, hence the essence of choosing controls that are suitable for the FIPS 200 program and standard publication 800-53 of NIST.

Original source

There is the selection process whereby, after users defining the information that is important, they are required to choose the controls that are suitable for the program depending on standard publication 800-53 of NIST in addition to FIPS 200

3 Student paper 75%

Student paper

Assessing involves preparation for responding through evaluation of probable risks of safety in addition to mitigation prioritization.

Original source

Assessing which involves being ready into responding through evaluation of probable safety risks in addition to having mitigation prioritized

1 Student paper 67%

Student paper

Automation ensures maintenance of the Security framework of the agency, as well as having the given violations rectified and preservation of the model that is least privileged.

Original source

Automation ensures that the security framework of an agency is maintained, the violations get rectified in addition to the model that is least privileged gets preserved

1 Student paper 63%

Student paper

Additionally, there is making sure that any data capable of being impacted as an event's part gets safeguarded through archiving, deleting in addition to archiving or having them migrated into places that are different.

Original source

Then there is making sure that information capable of being impacted during the occurrence gets safeguarded through getting deleted, archived as well as migrated into places that are different

3 Student paper 72%

Student paper

There is monitoring of the policies of security through automation and making sure that the organizations' cyber hygiene is safeguarded and also monitored.

Original source

Have the security policies monitored through automation and ensuring preservation and monitoring of organizations' cyber hygiene

5 Student paper 80%

Student paper

System's baseline Security Requirements include:

Original source

These baseline security requirements include

1 Student paper 65%

Student paper

Categorizing the systems of information whereby it is a phase that is administrative and understanding the organizations' awareness.

Original source

Characterizing the systems of information which is an administrative phase that needs the organizations' awareness

3 Student paper 77%

Student paper

Selection of management of security that indicates the controls for security are operational, technological in addition to administrative controls and techniques of prevention that are utilized within information system of the company, accountable for preserving security, the availability in addition to the systems integrity and information.

Original source

Choose security management whereby the safety controls are operational, administrative, and prevention techniques or technological controls utilized in the information system of the organization preserving the availability, security in addition to systems integrity and information

1 Student paper 85%

Student paper

Implementation of management of security whereby the third phase needs a firm to carry out controls of security and identification on the manner in which the control systems get utilized in the system of data in addition to operating setting.

Original source

Implementation of security management whereby the third phase needs a company to carry out security controls and identifying the manner in which the systems of control get utilized in the system of data in addition to its setting that is in operation

1 Student paper 76%

Student paper

Monitoring management of security enables the organization in retaining the clearance security of a system of data for a long duration within an operating setting that is changing rapidly where the systems make adjustments to vulnerabilities, threats, technology that are evolving and the processes of a business. Network Infrastructure baseline security include: Categorizing the system or framework in addition to the data that it gathers, keeps and transmits depending on the effective analysis.

Original source

There is also the monitoring of security management that enables an organization to have the data system security clearance retained for a period that is long within an operating setting that is changing rapidly whereby the systems get adjusted into the evolving vulnerabilities, threats, processes of business and technology (Shad, et.al, 2019) Baseline security of Network infrastructure Categorizing the system or framework in addition to the data that is gathered, stored and transmitted based on effective analysis

1 Student paper 92%

Student paper

Implementation of the measures of security and recording the manner in which the controls get implemented within the system as well as the operating surrounding.

Original source

Implementation of measures for security in addition to recording the manner in which the controls get implemented within a system as well as the operating surrounding

6 Student paper 64%

Student paper

Assessing the controls to utilize procedures that are appropriate in describing the validity which the systems of control are implemented appropriately.

Original source

Assess-security controls should appropriate procedures describing the weight in which the control systems are properly implemented

1 Student paper 62%

Student paper

Authorization whereby the operation program ends up focusing on the risk evaluation to the effectiveness of the organization and assets, individuals among other agencies and nation.

Original source

Authorization whereby operation of the program concentrates on the risk evaluation into the effectiveness of the organization and people, assets, different agencies and the nation which is as a result of the company implementation and the evaluation of the identified risk is suitable

3 Student paper 66%

Student paper

Monitoring and evaluation of system security policies that are chosen on a process that is continuous.

Original source

In addition to monitoring and evaluating chosen security policies system on a continuous procedure

7 Student paper 82%

Student paper

Information processing baseline

Original source

Baseline Security of Information Processing

3 Student paper 70%

Student paper

The framework for management of risk provides a structured, organized and plan that is responsible in identifying privacy and security risks, inclusive of the classification of information security.

Original source

Frameworks for risk management offer structured, organized and a plan that is responsive in identification of privacy and security risks inclusive of classification of regulate selection, information security, implementation and monitoring among others

1 Student paper 72%

Student paper

In addition, the framework also encourages strategic planning that is near-real-time and information system that is ongoing and control authorization via monitoring procedures that are continuous, offers the executives and senior managers with needed data for making decisions for managing risk that are efficient and cost effective.

Original source

In addition, RMF tends to encourage strategic planning that is neat real time and information system that is ongoing and control authorization that is common via monitoring procedures that are continuous, offering the executives and senior managers with the appropriate data for making decisions on management of risk that are cost effective and efficient in relation to the systems supporting their duties and functions of the business (Tasmin, et.al, 2020)

1 Student paper 76%

Student paper

The Risk management framework implementation connects crucial RMF at the risk management performance at the network level at the institution level.

Original source

The RMF assignments implementation connects important framework for management of risk during the network level to management of risk performance at the level of the organization

8 Student paper 66%

Student paper

Additionally, it offers transparency and accountability for performed controls through organizations' information systems.

Original source

It also offers transparency and responsibility for the controls performed in the company's information systems

3 Student paper 100%

Student paper

Fagan, M., Megas, K. N., Scarfone, K., & Smith, M.

Original source

Fagan, M., Megas, K N., Scarfone, K., & Smith, M

3 Student paper 100%

Student paper

IoT Device Cybersecurity Capability Core Baseline (No. NIST Internal or Interagency Report (NISTIR) 8259A). National Institute of Standards and Technology.

Original source

IoT Device Cybersecurity Capability Core Baseline (No NIST Internal or Interagency Report (NISTIR) 8259A) National Institute of Standards and Technology

9 Student paper 97%

Student paper

Security and key management in IoT-based wireless sensor networks: An authentication protocol using symmetric key. International Journal of Communication Systems, 32(16), e4139.

Original source

Security and Key Management in IoT Based Wireless Sensor Networks An Authentication protocol using Symmetric Key International Journal of Communication Systems 32.16

10 scpslab 84%

Student paper

A survey on internet of things security:

Original source

Karimipour, "Survey on Internet of Things Security

11 Student paper 72%

Student paper

Internet of Things, 100129.

Original source

Internet of Things

2 Student paper 100%

Student paper

Kumar, R., & Goyal, R.

Original source

Kumar, R., & Goyal, R

3 *Student paper*	100%
Student paper On cloud security requirements, threats, vulnerabilities and countermeasures:	Original source On cloud security requirements, threats, vulnerabilities and countermeasures

3 *Student paper*	100%
Student paper Computer Science Review, 33, 1-48.	Original source Computer Science Review, 33, 1-48