



Islington college
(इरिलिङ्टन कलेज)

CC5052NI Risk, Crisis & Security Management

50% Individual Coursework on Risk Management/Risk Control

**Semester 3
2024-25 Autumn**

Student Name: Sushant Chaudhary

London Met ID: 23047494

College ID: np01nt4a230169

Assignment Due Date: January 10, 2025

Assignment Submission Date: January 10, 2025

Submitted To: Akash Ojha

Count: 2166

I confirm that I understand my coursework needs to be submitted online via MST Classroom under the relevant module page before the deadline for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

**A Coursework Submitted
on
Risk Management/Risk Control**

**Semester 3
2024-25 Autumn**

Student Name: Sushant Chaudhary

London Met ID: 23047494

College ID: np01nt4a230169

Assignment Due Date: January 10, 2025

Assignment Submission Date: January 10, 2025

Submitted To: Akash Ojha

Count: 2166

Acknowledgement

I would like to express my deepest gratitude to my teachers, Mr. Akash Ojha and Mr. Apil Chand, for their inestimable guidance, stimulant, and support throughout the completion of this coursework on Risk Management in Cybersecurity A Case Study on the Colonial Pipeline Ransomware Attack (2021). Their moxie and perceptive feedback have been necessary in suiting the instruction and quality of this report.

I'm also thankful for the resources and mastering openings handed by the intellectual context at my institution, which have significantly contributed to the prosperous completion of this work. Finally, I extend my estimation to my peers and line for their nonstop brace and provocation throughout this trip.

Thank you all for your unwavering backing and belief in my capacities.

Sincerely,

Sushant Chaudhary

23047494_SUSHANT CHAUDHARY.docx

 Islington College, Nepal

Document Details

Submission ID

trn:oid::3618:78718674

Submission Date

Jan 9, 2025, 9:10 PM GMT+5:45

Download Date

Jan 9, 2025, 9:12 PM GMT+5:45

File Name

23047494_SUSHANT CHAUDHARY.docx

File Size

16.7 KB

14 Pages

2,291 Words

14,452 Characters







Page 1 of 19 - Cover Page

Submission ID trn:oid::3618:78718674




13% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

-  **24 Not Cited or Quoted 11%**
Matches with neither in-text citation nor quotation marks
-  **5 Missing Quotations 2%**
Matches that are still very similar to source material
-  **0 Missing Citation 0%**
Matches that have quotation marks, but no in-text citation
-  **0 Cited and Quoted 0%**
Matches with in-text citation present, but no quotation marks

Top Sources

- 2%  Internet sources
- 2%  Publications
- 12%  Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Abstract

Risk management plays a pivotal role in ensuring the security, resilience, and continuity of modern organizations. This report explores the application of the ISO 31000 framework, a globally recognized standard for risk management, and its significance in addressing cybersecurity challenges. Using the Colonial Pipeline ransomware attack of 2021 as a case study, the report identifies critical risk management failures, such as inadequate risk identification, poor threat treatment, and insufficient monitoring. It highlights the lessons learned from the incident and provides actionable recommendations for organizations to strengthen their risk management strategies. Through a detailed analysis of ISO 31000, the report emphasizes the importance of a structured and proactive approach to mitigating risks. The findings underscore the value of integrating risk management into organizational governance and culture, ensuring ongoing adaptability to an ever-evolving threat landscape. This study aims to empower organizations to adopt ISO 31000 principles for enhanced security and operational excellence.

Table of Contents

Acknowledgement	i
Abstract.....	iv
Table of Figures	vi
List of abbreviations	vii
1. Introduction.....	1
1.1 Background and Context	1
1.2 Rationale	1
1.3 Aim and Objectives	2
2. Literature Review.....	3
2.1 Overview of Risk Management Concepts	3
2.1.1 Overview of ISO 31000	3
2.2 Risk operation Process in ISO 31000.....	3
2.4 Risk Control Techniques.....	6
3. Case Study: Colonial Pipeline Ransomware Attack (2021).....	8
4. Issues Identification, Analysis, and Reflection.....	9
4.1 Challenges in enforcing ISO 31000	9
4.2 Reflection	10
5. Conclusion	12
6. References	13

Table of Figures

Figure 1: ISO 31000 Risk Management Process	5
Figure 2:Common Risk Control Strategies (Scrut Automation, 2023)	7
Figure 3:Timeline of the Colonial Pipeline Attack (DiMaggio, 2022)	8
Figure 4:Visual representation of cybersecurity risk management failures (Ardoq, 2024).....	10
Figure 5:Challenges and solutions in implementing ISO 31000 (slideteam, 2024)	11

List of abbreviations

Abbreviation	Full Form
CISA	Cybersecurity and Infrastructure Security Agency
ISO	International Organization for Standardization
IT	Information Technology
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
OT	Operational Technology
SGS	General Society of Surveillance
CISO	Chief Information Security Officer

1. Introduction

1.1 Background and Context

Risk management refers to the process of identifying, laying, and managing risks that could negatively affect an organization. In cybersecurity, risk management focuses on identifying, helping, and mitigating risks associated with digital structure, data breaches, and cyber threats. In the moment's connected world, the significance of operative risk management is lesser than ever, especially with the growing trouble of cyberattacks, ransomware, and data breaches. Organizations must have visionary strategies to deal with pitfalls ranging from financial to reputational, especially as technology continues to evolve and introduce new weakness (ISO 31000, 2018) (NIST, 2024).

Risk control, on the other hand, involves enforcing measures to reduce or exclude risks identified during the risk operation process. Common threat control strategies include threat avoidance, threat mitigation, threat transfer, and threat acceptance. These strategies form the backbone of an association's overall approach to security and functional durability.

The need for strong risk management and control measures has come decreasingly apparent with the rise of high- profile cybersecurity incidents. The 2021 Colonial Pipeline ransomware attack serves as a high illustration of the consequences of shy risk management practices and highlights the critical need for associations to borrow a visionary station on cybersecurity and risk management (ZenGRC Team , 2024).

1.2 Rationale

In an era of rapid-fire technological advancement and adding cyber threats, businesses must remain graceful in their risk operation efforts. Organizations that fail to manage pitfalls meetly may face severe consequences, including financial losses, reputational damage, and legal ramifications. The explanation behind fastening on threat operation and control is to understand the stylish practices, fabrics, and ways available to associations and insure they're adequately defended. By enforcing applicable threat control measures, businesses can reduce their exposure to pitfalls and minimize the impact of implicit pitfalls.

Likewise, risk management is integral to building organizational adaptability and icing that companies can recover from unanticipated disturbances. As seen in the fate of the Colonial Pipeline attack, an association's capability to snappily recover from a cyberattack can significantly impact its functional durability and long- term success. Thus, a comprehensive approach to threat operation not only involves relating and mitigating risks but also icing the company is equipped to manage heads when they occur.

1.3 Aim and Objectives

Aim

The aim of this report is to research the significance of threat management and risk control in current associations, particularly within the department of cybersecurity, and to give insights and practicable recommendations to help associations navigate and mitigate risks effectively.

The primary objectives of this report are

1. To examine the role of risk management and control in the environment of cybersecurity and business operations.
2. To explore colorful risk management structures and ways, assessing their effectiveness.
3. To reflect on the challenges faced by associations in applying risk control measures and strategies.
4. To give practicable recommendations for associations looking to enhance their risk management practices.

2. Literature Review

2.1 Overview of Risk Management Concepts

Risk management is an organized approach to Evaluating and overseeing dangers that might adversely affect organization objectives.

2.1.1 Overview of ISO 31000

ISO 31000 is a worldwide recognized measure that gives rules for overseeing dangers in associations. It emphasizes the integration of threat operation into governance, program, and missions. The framework is aimed to be adaptable across diligence and encourages associations to

- Establish a structured path to risk management.
- Embed risk management into organizational accomplishment.
- ensure accountability and transparency in decision- making (ISO 31000, 2018).

The framework's principles carry creating value, being inclusive, and esteeming human and artistic factors. It provides a nonstop process for identifying, assessing, and responding to risks, making it largely workable to dynamic surroundings like cybersecurity.

2.2 Risk operation Process in ISO 31000

The ISO 31000 frame outlines a structured process for threat operation:

- **Establishing the Context:** This step involves defining the internal and external environments where the association operates. It includes gathering the association's aims, stakeholder prospects, governmental conditions, and the operational landscape. This environment provides the foundation for relating and managing risks effectively.
- **Risk Identification:** The association identifies implicit risks that could impact its objects. This involves feting threats, weakness, and opportunities. Common or garden styles carry brainstorming sessions, geek dissection, and reviewing literal data to discover sources of threat.
- **Risk Analysis:** Each identified threat is anatomized to determine its liability of being and the implicit impact it might have. Quantitative or qualitative methods may be exercised, depending on the complication and nature of the pitfalls. This dissection helps to understand the inflexibility of risks and their implicit consequences.

- **Risk Evaluation:** Once risks are anatomized, they're prioritized based on their significance to the association. This evaluation helps in determining which risks challenge immediate concentration, which can be covered, and which can be accepted. Prioritization ensures resources are distributed efficiently to manipulate the most overcritical risks.
- **Risk Treatment:** This step focuses on developing and enforcing strategies to take the linked risks. Strategies include
 - **Mitigating risks:** Reducing the liability or impact of risks through preventative measures.
 - **Transferring risks:** participating or outsourcing risks, like taking insurance.
 - **Accepting risks:** Admitting certain risks that fall within respectable verges.
 - **Avoiding risks:** Changing processes or discontinuing conditioning to exclude risks mostly.
- **Monitoring and Review:** threat management is a nonstop process. Regular monitoring ensures pitfalls are pursued, and the effectiveness of enforced strategies is assessed. The review process allows associations to acclimatize to changes in the internal or foreign terrain and upgrade their threat management path.
- **Message and Consultation:** Engaging stakeholders throughout the process ensures translucency and builds trust. Operating message facilitates collaboration, enhances resolution-timber, and ensures that everyone involved understands the risks and their places in mollifying them.



Figure 1: ISO 31000 Risk Management Process

2.3 Advantages of utilizing ISO 31000

- **Scalability:** ISO 31000 can be acclimatized to fit associations of all sizes and industries.
- **Inflexibility:** Its principles can be applied to varied threat types, involving cybersecurity, fiscal, and functional pitfalls.
- **Continuous enhancement:** The iterative nature of ISO 31000 ensures that risk operation strategies evolve with changing surroundings.

2.4 Risk Control Techniques

Risk control strategies are used to manage and mitigate the implicit impact of identified risks. Four primary categories of risk control ways are generally employed

1. Risk Avoidance: This strategy involves changing plans, procedures, or processes to avoid a threat altogether. For illustration, an association may decide not to borrow certain technologies or engage in business practices that carry high risks.

2. Risk Mitigation: Risk mitigation aims to reduce the probability or impact of pitfalls. Common cybersecurity trouble mitigation strategies include installing firewalls, using encryption to cover data, assuming multi-factor authentication (MFA), and administering intrusion discovery systems (IDS). These measures help lower the liability of an attack or degrade its harshness if it occurs.

3. Risk Transfer: Risk transfer involves shifting the responsibility for managing a trouble to a third party. For illustration, managing with cyber insurance can help alleviate the financial impact of a security breach. Outsourcing specific operations, analogous to data storehouse or handling sensitive deals, may also help reduce exposure to certain risks.

4. Risk Acceptance: In some cases, associations may decide to accept certain risks, particularly when the costs of mollifying the risk are more advanced than the implicit impact. Threat acceptance is frequently accompanied by a plan for monitoring and replying to the threat if it materializes.

These risk control ways are not mutually exclusive and frequently need to be combined in a comprehensive approach to address the range of risks an association face. Given the evolving nature of cyber pitfalls, espousing a multi-pronged approach to risk operation combining mitigation, avoidance, and acceptance is crucial (Chatterton, 2024).

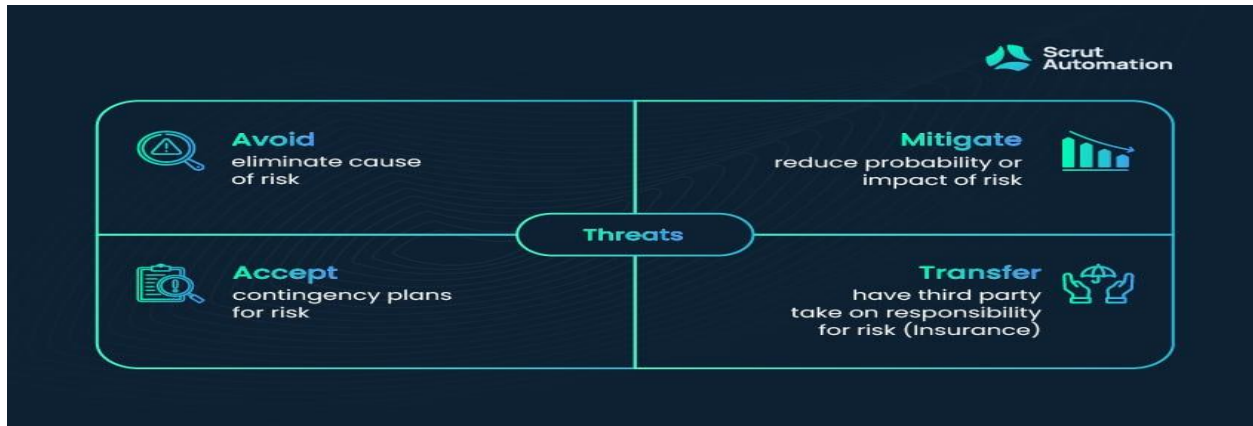


Figure 2: Common Risk Control Strategies (Scrut Automation, 2023)

3. Case Study: Colonial Pipeline Ransomware Attack (2021)

3.1 Overview of the Attack

The Colonial Pipeline ransomware attack in May 2021 marked one of the most significant cyberattacks on overcritical structure in the United States. The rush, carried out by the Darkside ransomware group, targeted the IT systems of Colonial Pipeline, which operates one of the largest energy channels in the U.S., supplying roughly 45 of the East Coast's energy.

The breach began with the concession of a single hand account word, which lacked multi-factor authentication (MFA). This access allowed the bushwhackers to emplace ransomware that translated sensitive business data, muscling the company to make down missions for closely a week. This led to wide energy scarcities, panic buying, and dislocations across multitudinous countries, causing profitable losses estimated in the hundreds of millions of bones. social Pipeline eventually paid a rescue of roughly\$ 4.4 million in Bitcoin, portion of which was latterly reacquired by law enforcement. (Easterly, 2024) (industrialcyber, 2023)

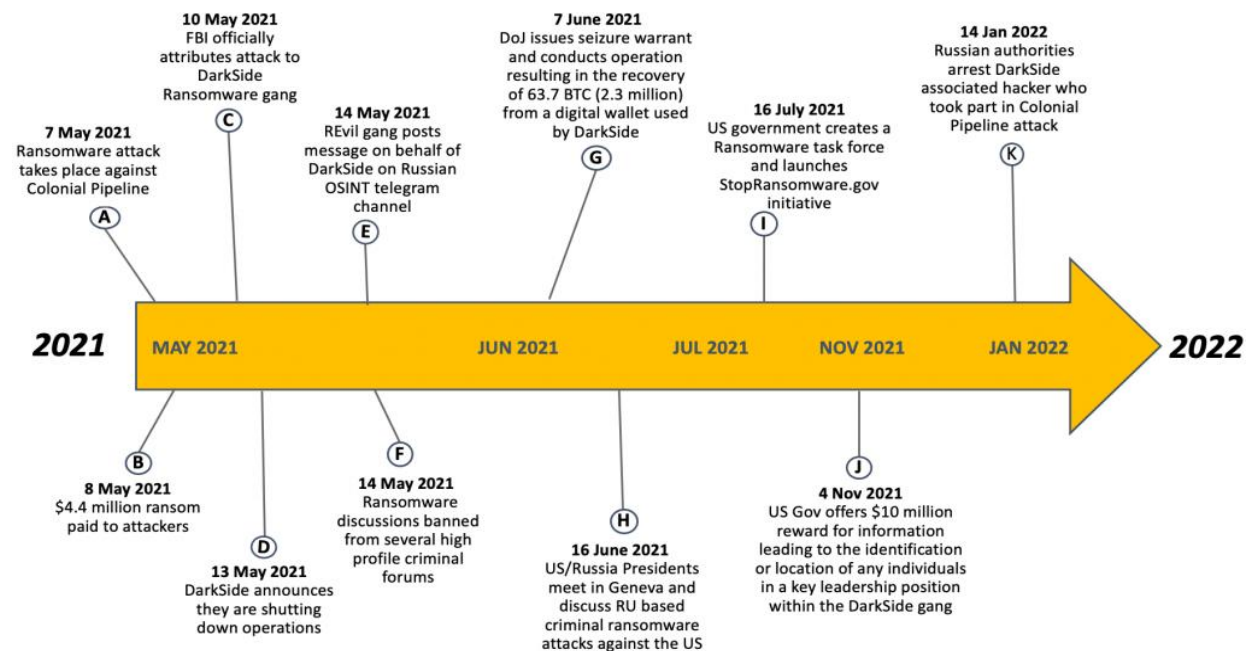


Figure 3: Timeline of the Colonial Pipeline Attack (DiMaggio, 2022)

4. Issues Identification, Analysis, and Reflection

4.1 Challenges in enforcing ISO 31000

Analyzing the Colonial Pipeline incident through the ISO 31000 frame highlights several failings in their threat operation processes:

- **Lack of Risk Identification:**

The association failed to exhaustively identify susceptibility in its IT systems, especially related to authentication mechanisms. For example, single- factor authentication on overcritical accounts posed a significant and operable threat that went along unnoticed.

- **Inadequate Risk Treatment:**

Precautionary measures such as multi-factor authentication (MFA) and network segmentation were moreover not enforced or rightly positioned. These measures could have significantly downgraded the collision of unauthorized access and side motion within the network.

- **Poor Monitoring and Review:**

The company demanded robust mechanisms for nonstop monitoring of cybersecurity controls and failed to modernize its defenses to manipulate evolving threats. As a result, the systems were left vulnerable to exploitation, despite growing mindfulness of ransomware threats.

- **Insufficient Communication and Consultation:**

The ISO 31000 principle of engaging stakeholders was not effectively applied. workers may not have entered acceptable cybersecurity training to recognize pitfalls, similar as phishing cracks, which are common or garden precursors to ransomware attacks. (Tahir, 2024) (Rotibi & saxena, 2024) (sgs, 2024)



Figure 4: Visual representation of cybersecurity risk management failures (Ardoq, 2024)

4.2 Reflection

The Colonial Pipeline attack provides a clear example of the importance of adopting a proactive and systematic approach to risk management, particularly for organizations operating critical infrastructure. Key lessons include:

- **Strengthening Risk Identification:**

Organizations should regularly achieve complete risk assessments to identify and estimate susceptibility. This includes maintaining a force of all IT means, laying their criticality, and prioritizing risks grounded on liability and implicit impact.

- **Implementing Robust Risk Treatment Plans:**

visionary measures such as MFA, zero- trust architecture, and segmentation of operational technology (OT) and IT networks are essential. Colonial Pipeline's dependence on outdated defenses underscores the significance of regularly upgrading and modernizing security controls.

- **Continuous Monitoring and Review:**

Real- time monitoring of systems and constant audits are vital for detecting and responding to threats beforehand. Employing automated tools for anomaly discovery and intrusion prevention can enhance an association's capability to alleviate risks.

- **Enhancing Cybersecurity Awareness and Training:**
workers play a overcritical part in maintaining cybersecurity. Regular training programs on feting phishing and other common attack vectors should be obligatory to reduce the threat of human error.
- **Improving Incident Response Preparedness:**
A well- outlined and rehearsed incident response plan is key for minimizing the impact of attacks. Colonial Pipeline's delayed reaction suggests the absence of such a plan or inadequate preparation.
- **Engaging with External Stakeholders:**
Collaboration with government agencies, industry groups, and cybersecurity experts is critical for understanding emerging threats and sharing best practices. Organizations can benefit from participating in information-sharing initiatives such as the Cybersecurity and Infrastructure Security Agency (CISA). (Monken & Smith, 2021)

Challenges of implementing ISO 31000 standard

This slide defines that implementing the ISO 31000 standard faces challenges such as continuous effort, potential false security, and risk aversion, impacting organizational resilience and adaptability.



This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Figure 5: Challenges and solutions in implementing ISO 31000 (slideteam, 2024)

5. Conclusion

Effective risk management is no longer an elective but a overcritical necessity for ultramodern associations operating in an decreasingly connected and unpredictable digital geography. This report has featured the value of the ISO 31000 frame as a robust and adaptable guideline for relating, assaying, and mollifying risks. The Colonial Pipeline ransomware attack of 2021 pointed out the destructive consequences of inadequate risk management, emphasizing the want for a visionary, structured path to threat valuation and treatment.

By espousing ISO 31000 principles, associations can establish a flexible foundation for managing pitfalls, icing not only the security of means and missions but also the safekeeping of stakeholder trust and organizational character. The frame's emphasis on integration into governance, nonstop enhancement, and stakeholder engagement ensures that pitfalls are played holistically and effectively through all situations of the association.

The challenges of resource constraints, fleetly evolving threats, and defiance to revise are real and significant. Still, these expostulations can be managed through strong leadership, investment in training and mindfulness, and using ultramodern technologies to enhance monitoring, discovery, and reaction capabilities.

In conclusion, the relinquishment of ISO 31000 empowers associations to navigate sophisticated risk geographies with confidence. Through harmonious operation and iterative refinement of risk operation strategies, associations can't only reduce susceptibility but also transfigure threat into openings for excrescency, invention, and sustained functional distinction. It's imperative for companies to feel that threat operation is a nonstop trip, not a destination, and those that prioritize it'll be better fitted to thrive in the face of query.

6. References

- Easterly, J. (2024, december 25). *cisa*. Retrieved from cisa: <https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years>
- Ardoq. (2024, december 20). *Ardoq*. Retrieved from Ardoq: <https://www.ardoq.com/blog/cybersecurity-risk-mitigation>
- Chatterton, C. (2024, august 13). *hyperproof.io/*. Retrieved from hyperproof.io/: <https://hyperproof.io/resource/risk-management-techniques/>
- industrialcyber. (2023, may 06). *industrialcyber*. Retrieved from industrialcyber: <https://industrialcyber.co/critical-infrastructure/critical-infrastructure-continues-to-call-for-more-attention-two-years-after-colonial-pipeline-ransomware-attack/>
- ISO 31000. (2018). *iso.org*. Retrieved from iso.org: <https://www.iso.org/obp/ui/en/#iso:std:65694:en>
- Monken, J., & Smith, M. (2021, 06 01). *mwi.westpoint*. Retrieved from mwi.westpoint: <https://mwi.westpoint.edu/the-colonial-pipeline-hack-shows-we-need-a-better-federal-cybersecurity-ecosystem/>
- NIST. (2024, February 26). *nist.gov*. Retrieved from nist.go: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
- Rotibi, A., & saxena, n. (2024, november 17). *ietresearch*. Retrieved from ietresearch: <https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/cps2.12105>
- Scrut Automation. (2023, october 04). *Scrut Automation*. Retrieved from scrut.io: <https://www.scrut.io/post/risk-management-techniques>
- sgs. (2024, december 25). *sgs*. Retrieved from sgs: <https://www.sgs.com/en-id/news/2024/10/iso-31000-2018-risk-management-boosting-profitability-and-business-sustainability>
- slideteam. (2024, december 20). *slideteam*. Retrieved from slideteam.net: <https://www.slideteam.net/challenges-of-implementing-iso-31000-standard-mastering-risk-management-risk-ss.html>
- Tahir. (2024, december 25). *medium*. Retrieved from medium: <https://medium.com/@tahirbalarabe2/my-experience-working-with-iso-31000-risk-management-frameworks-ca7557b99a5f>

ZenGRC Team . (2024, august 30). *ZenGRC* . Retrieved from ZenGRC Team . :
<https://www.zengrc.com/blog/risk-control-risk-management-whats-the-difference/>