Raytheon Defense Contractor Risk Management Plan (CYS-310 Project)

Ben Acuff & Ben Molloy

1. Introduction 4
2. Scope 4
2.1 Tangible and Intangible Assets Overview 4
3. Assets 7
3.1 Detailed Asset List 7
4. Cost Benefit Analysis 9
4.1 Asset Value Assessment 9
5. Compliance Laws and Regulations 11
6. Key Roles and Responsibilities 12
7. Risk Assessment 14
7.1 Introduction 14
7.2 Scope 14
7.3 Boundaries 15
7.4 Assets and Activities 15
7.4.1 Tangible Assets List 15
7.4.2 Intangible Assets List 16
7.4.3 Data Center Assets and Activities 16
7.4.3.1 Tangible Assets List (Data Center) 16
7.4.3.2 Intangible Assets List (Data Center) 16
7.5 Threats and Vulnerabilities 17
7.5.1 Tangible Assets 17
7.5.2 Intangible Assets 19
7.5.3 Risk Matrix Graph 20
7.6 Types of Controls 22
7.7 Key Roles & Responsibilities 24
7.8 Proposed Schedule 26

7.8.1 Timeline Table 26
8. Risk Mitigation Plan 28
8.1 Introduction 28
8.2 Scope 28
8.3 Boundaries 29
8.4 Risk Mitigation Strategies 29
8.5 Controls and Policies 33
8.5.1 Security Control and Policy List 33
8.6 Monitoring and Evaluation 36
8.6.1 Key Performance Indicators (KPI) 36
8.6.1.1 KPI Table: Objectives and Measurements 36
8.6.2 Continuous Improvement Plan 37
8.6.2.1 Four Points of Continuous Improvement 37
8.6.3 Reporting Mechanisms 38
8.6.4 Vulnerability & Exploit Assessment Strategies 39
8.6.4.1 Vulnerability Assessment Strategies List 39
8.6.4.2 Exploit Assessment Strategies List 41
8.7 Conclusion 42
9. BIA & BCP Plan 43
9.1 Introduction 43
9.2 Business Impact Analysis (BIA) 43
9.2.1 Critical Business Functions (CBF) 43
9.2.2 Critical Resources (CR) 44
9.3 Maximum Acceptable Outage (MAO) and Impact 44
9.4 Recovery Point Objective (RPO) and Recovery Time Objective (RTO) 46
9.5 Business Continuity Plan (BCP) 46
9.5.1 Notification/Activation Phase 47
9.5.2 Recovery Phase 47
9.5.3 Reconstruction Phase 47

9.5.4 Plan Training, Testing, and Exercising Phase 48
9.6 Cost-Benefit Analysis (CBA) 48
9.6.1 Cost to Implement Recommendations 49
9.6.2 Projected Benefits 49
9.6.3 Control Factor 50
9.6.4 Summary 51
9.7 Conclusion 52

1. Introduction

In the world of military contracting, Raytheon stands as a steadfast symbol of innovation and precision. With a storied history spanning decades, Raytheon has consistently delivered cutting-edge solutions that have reshaped national security and technology. This Risk Management Plan (RMP) embodies Raytheon's unwavering commitment to protecting its operations, preserving its invaluable assets, and ensuring the continuity of its mission-critical functions as a leading military contractor.

Raytheon's journey as a military contractor is deeply intertwined with its dedication to providing essential defense technologies that empower nations to secure their interests. The company's legacy of excellence is a testament to its ability to navigate the intricate landscape of military contracting, where accuracy, reliability, and adaptability are paramount.

2. Scope

The scope of this Risk Management Plan covers the spectrum of Raytheon's military contracting operations, encompassing both tangible and intangible assets. Raytheon's diverse range of assets reflects its global reach and commitment to advancing defense technologies.

2.1 Tangible and Intangible Assets Overview

On the tangible front, Raytheon's assets include a network of cutting-edge manufacturing facilities positioned worldwide. These facilities serve as hubs of innovation, where advanced defense technologies are crafted to meet the ever-evolving needs of modern defense. Complementing this infrastructure are Research and Development

(R&D) Centers where top-tier talent collaborates to create, develop, and refine military solutions that redefine the industry.

Raytheon's highly skilled workforce forms the backbone of its tangible assets, with experts in various fields driving the company's innovations. Information Systems underpin its operations, facilitating seamless communication, collaboration, and data management, all vital to successful military contracting. The robust supply chain and logistics infrastructure ensure the reliable delivery of essential components and materials, critical to meeting military contracting deadlines.

Raytheon's expertise spans various domains, including aircraft systems, missile systems, electronics and sensors, naval systems, space technologies, satellite systems, and more, all tailored to meet the exacting requirements of military contracting.

Complementing these tangible assets are intangible resources of paramount importance. Raytheon's defense technologies, often proprietary and classified, form the foundation of its capabilities in military contracting. The company's intellectual property portfolio safeguards its innovations, while contracts and agreements provide the basis for its engagements with governments and defense organizations worldwide.

In an increasingly connected world, cybersecurity capabilities are indispensable for safeguarding sensitive data and operations, a vital component of Raytheon's military contracting activities. Furthermore, Raytheon's global network of clients and partners spans the globe, requiring adept management to ensure robust relationships and mutual success in the competitive arena of military contracting.

Raytheon's stellar track record is further underscored by impressive statistics, including an amount obligated of $12.3 billion across 10,000 contracts. With a workforce of 61,000 employees, Raytheon is at the forefront of military contracting. The company's current work includes a $31.8 million contract for 464 Excalibur extended-range precision projectiles, a testament to its technological prowess. Using its GPS capabilities, the Excalibur is considered to be the longest-range, most precise, cannon-fired projectile in the world.

In this context, this Risk Management Plan reflects Raytheon's commitment to prudently address the unique challenges and assets inherent to its role as a prominent military contractor. By effectively leveraging its tangible and intangible assets, Raytheon aims to mitigate risks, ensure business continuity, and continue its storied tradition of enhancing global security and technological progress in the realm of military contracting.

Key areas covered within the scope of this plan:

- Physical Security: Securing and protecting Raytheon’s physical assets, facilities, and data centers.
- Information Security: Keeping the confidentiality, integrity, and availability of Raytheon’s sensitive data, intellectual property, and other classified information.
- Network Security: Securing and protecting Raytheon’s communication systems, internally and externally, to defend against any cyberthreats.
- Compliance: Adhering to any laws, regulations, and industry standards in the defense and military vendor sectors.

- Vendor Risk Management: Managing the risks associated with third-party vendors and suppliers is essential, given that their services might overlap with Raytheon's operations.

3. Assets

Raytheon's leadership in military contracting is rooted in a comprehensive array of assets, both tangible and intangible, that are integral to its operations. In the realm of tangible assets, the company boasts a global network of advanced manufacturing facilities and innovative Research and Development (R&D) Centers, underpinned by a highly skilled and dynamic workforce. These tangible assets are further supported by a robust Information Systems infrastructure, facilitating seamless communication and data management. Raytheon also maintains a dependable supply chain and logistics setup to ensure the timely delivery of critical components and materials. The company's expertise spans a diverse range of domains, encompassing aircraft systems, missile systems, electronics and sensors, naval systems, space technologies, satellite systems, aircraft carriers (if applicable), and land-based defense systems, each meticulously tailored to meet the intricate demands of modern military contracts.

3.1 Detailed Asset List

Complementing these tangible assets are intangible resources of equal significance. Proprietary defense technologies, often classified, provide Raytheon with a competitive edge, while intellectual property protections safeguard these innovations. Contracts and agreements serve as the foundation for collaborative partnerships with governments and defense organizations worldwide. In an era where cybersecurity is paramount, Raytheon's capabilities in this domain are exceptional, ensuring the

safeguarding of sensitive data and operations. Lastly, the company's extensive global network of clients and partners spans the globe, necessitating adept management to foster strong relationships and ensure mutual success in the highly competitive landscape of military contracting.

All of these assets can be seen in the following list view:

Tangible Assets

- Manufacturing Facilities
- Research and Development (R&D) Centers
- Skilled Workforce
- Information Systems
- Supply Chain
- Logistics Infrastructure
- Aircraft Systems
- Missile Systems
- Electronics and Sensors
- Naval Systems
- Space Technologies
- Satellite Systems
- Aircraft Carriers (if applicable)
- Land-Based Defense Systems

Intangible Assets

- Defense Technologies

- Intellectual Property
- Contracts and Agreements
- Financial Resources
- Cybersecurity Capabilities
- Global Network of Clients

4. Cost Benefit Analysis

Conducting a cost benefit analysis is essential for evaluating the financial viability and overall impact of Raytheon's operations. This analysis takes into account the company's investments, expenses, and returns across various facets of its business.

4.1 Asset Value Assessment

Investments:

Raytheon allocates substantial investments into its tangible and intangible assets. Tangible investments encompass the establishment and maintenance of manufacturing facilities, R&D Centers, and Information Systems infrastructure. These require significant capital for construction, equipment, and ongoing operational costs. Additionally, the workforce represents a substantial investment in terms of salaries, benefits, and training.

Intangible investments include research and development expenses, cybersecurity infrastructure, and intellectual property protection. These investments aim to maintain technological leadership, safeguard sensitive information, and ensure compliance with legal requirements.

Expenses:

Operating costs are a significant component of Raytheon's expenses. These include manufacturing, supply chain, logistics, and workforce management expenses. Information Systems maintenance, cybersecurity measures, and legal compliance efforts also contribute to the company's expenses.

Returns and Benefits:

Raytheon's returns and benefits manifest in various ways. Tangible assets, such as manufacturing facilities and R&D Centers, lead to the development and production of high-value defense technologies, resulting in contract revenue. A skilled workforce contributes to innovation and project execution, enhancing the company's reputation and competitiveness.

Intangible assets yield returns through proprietary defense technologies, intellectual property monetization, and successful contract execution. Effective cybersecurity safeguards sensitive data and operations, mitigating potential financial losses due to security breaches.

Raytheon's global network of clients and partners generates substantial revenue through contract awards, demonstrating the financial benefits of its extensive operations.

Cost Benefit Assessment:

To assess the cost benefit, Raytheon evaluates its investments against returns and benefits. The return on investment (ROI) for tangible assets considers contract revenue generated by manufacturing facilities and R&D Centers. For the workforce, ROI is measured by project success rates and reputation enhancement.

Intangible assets' ROI includes revenue generated from proprietary technologies and intellectual property monetization. Effective cybersecurity reduces the financial impact of potential security breaches. The global network of clients and partners contributes to revenue through successful contracts.

Costs are weighed against these returns to determine the overall financial health of the company. The assessment allows Raytheon to make informed decisions regarding resource allocation, asset management, and risk mitigation strategies.

In conclusion, Raytheon's cost benefit analysis is a crucial tool for evaluating the financial impact of its investments and operations. This analysis enables the company to optimize its resource allocation, maximize returns, and maintain its position as a leader in military contracting.

5. Compliance Laws and Regulations

Raytheon must adhere to any compliance laws and regulations that it is subject to.

5.1 Applicable Laws and Regulations

1. Federal Information Security Modernization Act (FISMA): FISMA requires Raytheon to develop, document, and implement information security programs to protect information and information systems. FISMA applies to Raytheon as they provide services to federal agencies. [6]
2. National Industrial Security Program (NISP): NISP establishes security standards and procedures for handling classified information. NISP ensures the safeguarding of classified information between Raytheon and the U.S. government and military. [7]

3. Defense Federal Acquisition Regulation Supplement (DFARS): DFARS enforces cybersecurity requirements handling Department of Defense (DoD) information. DFARS applies to Raytheon as they handle DoD information. [4]
4. International Traffic in Arms Regulations (ITAR): ITAR establishes controls with the export and import of defense-related items and services that appear on the U.S. Munitions List. [8]
5. Federal Acquisition Regulation (FAR): FAR, also known as the “Bible” for government contracting [9], are rules and procedures that apply to any federal government contractor. [5]
6. Export Administration Regulations (EAR): EAR are regulations controlled by the U.S. Department of Commerce and U.S. Department of State to regulate “dual-use” items. These goods and any related data are items that are made for commercial use but have military applications. [1]
7. Foreign Corrupt Practices Act (FCPA): FCPA prohibits the payments of bribes to foreign officials to assist in obtaining or retaining business. [2]

6. Key Roles and Responsibilities

1. Chief Information Security Officer (CISO): The CISO is responsible for the overall cybersecurity posture and strategies of Raytheon. Responsibilities include, but are not limited to, managing the cybersecurity team, reporting to senior management, and oversight of risk assessment and mitigation.
2. Senior Management: Senior Management is responsible for all organizational risk, including information technology (IT). They develop strategies associated with risk

and risk management. Assigns and manages risk management responsibilities throughout the organization.

3. Information Technology Department (IT): The IT department is responsible for identifying and assessing the IT infrastructure and applications. They are also responsible for implementing security measures and controls.
4. System and Information Owners: System and Information Owners are responsible for ensuring that proper controls are in place. They are also responsible for any changes to the IT systems. They deny and approve changes to systems. This team also must understand the risk management process and support it if necessary.
5. Vendor Management Team: The vendor management team is responsible for monitoring third-party vendors and suppliers. They conduct regular audits and assessments of vendor security controls. [3]
6. Functional Management Team: The functional management team ensures business operations are efficiently managed daily. They make trade-off decisions regarding system security. Having a functional management team enables the achievement of risk management goals.
7. Information Security (IS) Management: The information security management team includes IT security program managers and cybersecurity specialists. They are responsible for Raytheon's security program, including risk management. They help identify, evaluate, and minimize risk. IS management acts as consultants.
8. Compliance Team: The compliance team will ensure that Raytheon remains in compliance with all laws, regulations, and contractual obligations.

9. Legal Department: The legal department handles legal issues related to risk management including ensuring policy compliance, managing insurance, and handling legal actions in risk management.
10. Security Awareness Trainers: Provides training to the users of IT systems throughout Raytheon. They develop training materials and plans. They are also responsible for incorporating risk assessment into training.
11. Insider Threat (Counterspy) Team: The insider threat team is responsible for identifying and assessing insider threats. Since Raytheon is a military vendor, insider threats pose an extreme risk to the confidentiality of our systems and information.

7. Risk Assessment

7.1 Introduction

The purpose of this risk assessment plan is to evaluate and prioritize risks that could impact Raytheon's military contracting operations. By comparing the likelihood and potential impact of specific threats, we can estimate the importance of addressing each threat. The following risk assessment will allow our organization, Raytheon, to allocate its resources appropriately, prioritize risk mitigation strategies, and ensure the success of its operations in the military contracting world.

7.2 Scope

This risk assessment covers a wide range of risks associated with Raytheon's military contracting operations. Not only does it encompass Raytheon's data center assets and activities, but it also extends to other areas. These areas include production and supply chain, research and development, logistics, and intangible assets such as

intellectual property (IP), contracts, and client relationships. This extensive scope ensures that no crucial act of our organization's business is overlooked when assessing risks.

7.3 Boundaries

The boundaries of this risk assessment focus on tasks directly related to Raytheon's military contracting operations. Any risks that fall outside of this context, such as those associated with a non-military business classification, will not be included. These boundaries are set so that the assessment remains aligned with Raytheon's primary mission, which is to create, innovate, and provide defensive solutions.

7.4 Assets and Activities

The following assets and activities are crucial to Raytheon's military contracting operations and are subject to assessment.

7.4.1 Tangible Assets List

1. Manufacturing Facilities
2. Research and Development (R&D) Centers
3. Skilled Workforce
4. Information Systems
5. Supply Chain
6. Logistics Infrastructure
7. Aircraft Systems
8. Missile Systems
9. Electronics and Sensors

10. Naval Systems
11. Space Technologies
12. Satellite Systems
13. Aircraft Carriers (if applicable)
14. Land-Based Defense Systems

7.4.2 Intangible Assets List

1. Defense Technologies
2. Intellectual Property
3. Contracts and Agreements
4. Financial Resources
5. Cybersecurity Capabilities
6. Global Network of Clients

7.4.3 Data Center Assets and Activities

The following listed content is specified for Raytheon's data centers.

7.4.3.1 Tangible Assets List (Data Center)

1. Data Centers
2. Server Hardware
3. Networking Infrastructure
4. Uninterruptible Power Supplies (UPS)
5. Cooling Systems
6. Security Systems

7.4.3.2 Intangible Assets List (Data Center)

1. Data Center Operations Expertise
2. Data Center Redundancy

3. Vendor Risk Management
4. Capacity Planning
5. Data Encryption Protocols
6. Incident Response Plan

7.5 Threats and Vulnerabilities

This risk assessment considers numerous potential threats and vulnerabilities that could affect Raytheon's military contracting operations. Below is a list of currently identified threat events and their associated risks, taking into account the newly added assets and activities in the data center domain.

7.5.1 Tangible Assets

1. Manufacturing Facilities:
    - Operational Risk: Risks related to the interruption of manufacturing due to natural disasters, accidents, or equipment failures are of high concern. Strategies such as disaster recovery plans and equipment maintenance schedules should be implemented.
2. Research and Development (R&D) Centers:
    - Intellectual Property Risk: Theft or compromise of sensitive R&D data can lead to intellectual property theft. This risk can be mitigated by stringent access controls, encryption, and regular security audits.
3. Skilled Workforce:
    - Talent Retention Risk: Ensuring that key employees remain with the company is essential. Strategies include competitive compensation

packages, professional development opportunities, and a supportive work environment.

4. Information Systems:
    - Cybersecurity Risk: Data breaches or cyberattacks can compromise sensitive information and disrupt operations.
5. Supply Chain:
    - Supply Chain Disruption Risk: Risks related to geopolitical issues, natural disasters, or logistical challenges disrupting the supply chain can be mitigated through supply chain diversification and the development of contingency plans.
6. Logistics Infrastructure:
    - Logistics Disruption Risk: Issues with transportation and logistics can lead to delays in product delivery. Measures such as route diversification, improved transport security, and contingency plans can mitigate these risks.
7. Aircraft Systems, Missile Systems, Electronics and Sensors, Naval Systems, Space Technologies, Satellite Systems, Aircraft Carriers, Land-Based Defense Systems:
    - Technology and Product Obsolescence Risk: Rapid advancements in technology may render existing systems obsolete. To mitigate this risk, Raytheon should invest in research and development for next-generation systems.
8. Data Center:

- Data Center Security Risk: Threats related to the security and availability of data center assets, including server hardware and networking infrastructure, need to be addressed. Security measures such as intrusion detection systems, access controls, and disaster recovery plans are crucial to protect data center assets and maintain continuity.

7.5.2 Intangible Assets

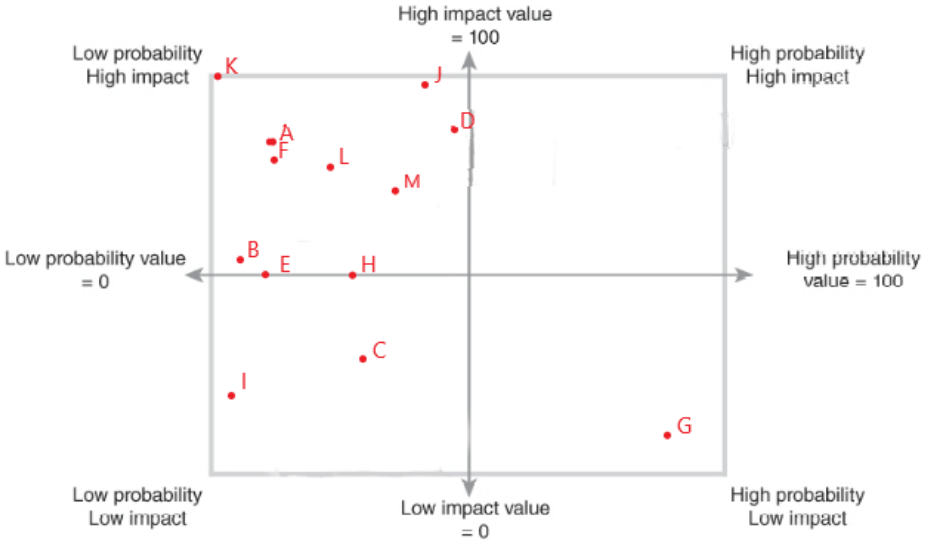
1. Defense Technologies:
    - Competitive Risk: Other companies may develop similar technologies, leading to increased competition. The emergence of rival technologies requires a continuous focus on innovation and competitive positioning.
2. Intellectual Property:
    - Intellectual Property Infringement Risk: Risk of infringement claims or disputes with other companies over patents or copyrights can be mitigated through patent monitoring, legal assistance, and dispute resolution mechanisms.
3. Contracts and Agreements:
    - Contractual Risk: Breach of contracts, disputes, or changes in government procurement policies can affect revenue streams.
4. Financial Resources:
    - Financial Market Risk: Economic downturns or market volatility can impact the company's financial stability. Diversified investments and fiscal responsibility are strategies for addressing this risk.
5. Cybersecurity Capabilities:

- Cybersecurity Risk: Failure to protect critical cybersecurity assets, including those within data centers, can result in data breaches and reputational damage. Regular penetration testing, employee training, and proactive threat monitoring are key strategies for addressing the risk of data breaches and cyberattacks.

6. Global Network of Clients:
    - Geopolitical Risk: Changes in international relations or conflicts can affect relationships with global clients. Diversifying client bases and maintaining international relationships are ways to mitigate the risk associated with changes in geopolitics.

7.5.3 Risk Matrix Graph

See Figure 1 on the next page, Raytheon RMP Risk Matrix Graph with Key Values.



Tangible

A) Operational Risk: Disruptions in manufacturing due to natural disasters, accidents, or equipment failures can impact production.

B) Intellectual Property Risk: Theft or compromise of sensitive R&D data can lead to intellectual property theft.

C) Talent Retention Risk: Losing key employees with specialized skills can hinder operations and innovation.

D) Cybersecurity Risk: Data breaches or cyberattacks can compromise sensitive information and disrupt operations.

E) Supply Chain Disruption Risk: Disruptions in the supply chain can impact production and delivery schedules.

F) Logistics Disruption Risk: Issues with transportation and logistics can delay product delivery.

G) Technology and Product Obsolescence Risk: Rapid advancements in technology may render existing systems obsolete.

Intangible:

H) Competitive Risk: Other companies may develop similar technologies, leading to increased competition.

I) Intellectual Property Infringement Risk: Risk of infringement claims or disputes with other companies over patents or copyrights.

J) Contractual Risk: Breach of contracts, disputes, or changes in government procurement policies can affect revenue streams.

K) Financial Market Risk: Economic downturns or market volatility can impact the company's financial stability.

L) Cybersecurity Risk: Failure to protect critical cybersecurity assets can result in data breaches and reputational damage.

M) Geopolitical Risk: Changes in international relations or conflicts can affect relationships with global clients.

Figure 1

7.6 Types of Controls

The risk management process will evaluate the effectiveness of various controls in mitigating the identified risks. Raytheon's controls include cybersecurity measures, disaster recovery plans, intellectual property protection strategies, supply chain management practices, and compliance measures. Security controls Raytheon will be implementing:

1. Access Control Policies:
    - Implement role-based access control (RBAC) to assign proper permissions based on job roles and responsibilities.
    - Use multi-factor authentication (MFA) for further user verification.
2. Network Security:
    - Implement firewalls and intrusion detection/prevention technologies to protect against unauthorized access and cybersecurity threats.
    - Regularly update and patch all network devices and access points to prevent vulnerabilities.
3. Data Encryption:
    - Encrypt all data at rest and in transit to prevent sensitive information or intellectual property leaks.
    - Use strong encryption protocols, such as AES (advanced encryption standard), for any communication channels and data storage systems.
4. Physical Security:
    - Secure physical facilities, data centers, and manufacturing facilities with access controls, surveillance systems, and intrusion alarms.

- Implement visitor access policies to control entry to protected areas.

5. Secure Software Development:
    - Implement secure coding practices into the software development workspaces to prevent vulnerabilities in applications.
    - Perform regular code reviews and software testing.
6. Security Monitoring and Logging:
    - Maintain comprehensive logs of all network and system activities.
    - Implement a Security Information and Event Management (SIEM) system to monitor traffic and detect security incidents.
7. Endpoint Security:
    - Use endpoint protection software to secure workstations and mobile devices.
    - Enforce device encryption policies for mobile devices.
8. Contractual and Legal Protection:
    - Develop contractual agreements that outline security requirements for contractors and business partners.
    - Ensure compliance with legal regulations and standards applicable to the military contracting sector.
9. Security Audits and Assessments:
    - Conduct regular security audits and assessments to evaluate the effectiveness of security controls in place and to identify areas of improvement.
10. Data Loss Prevention (DLP):
    - Deploy solutions to monitor and prevent unauthorized data transfers or leaks.

- Implement regular cloud data backups and other comprehensive tools for preventing data loss.

7.7 Key Roles & Responsibilities

To effectively manage and mitigate risks at Raytheon, a team of professionals play an essential role. These key individuals are involved in various aspects of the risk management and assessment process. They ensure the security, continuity, and success of Raytheon's military contracting operations. Below is a list of key roles and responsibilities within the organization:

1. Chief Information Security Officer (CISO):
    - Responsible for the oversight of all information security and managing Raytheon's security posture. Manages the implementation of security controls, risk assessments, and incident response.
2. Information Security Team:
    - Responsible for implementing and maintaining security controls, including access control policies, network security, data encryption, and endpoint security.
3. Physical Security Manager:
    - Responsible for ensuring the physical security of all facilities, data centers, and manufacturing facilities. This includes access controls, surveillance systems, and intrusion alarms.
4. Research and Development (R&D) Security Manager:

- Responsible for protecting all intellectual property (IP) and sensitive R&D data. This includes encryption, regular security audits, and access controls.

5. Incident Response Team:
    - Responsible for responding to security incidents and data breaches as outlined in Raytheon's incident response plan. This team is comprised of employees from various security departments within the organization.
6. Compliance Manager:
    - Responsible for ensuring that Raytheon complies with all legal regulations and standards applicable to military contracting, including business partner contracts.
7. Data Center Operations Team:
    - Responsible for managing and maintaining the confidentiality, integrity, and availability of all data center assets, including sever hardware, networking infrastructure, and other systems. This team also ensures data center storage, preventing redundancy and data capacity issues.
8. Cybersecurity Team:
    - Focuses on security the organization against cyber threats, ensuring data encryption protocols are in place, and conducting regular penetration testing and threat monitoring. This team also includes highly skilled researchers, staying up to date with even the newest cyber-attacks.
9. Legal and Intellectual Property Team:

- Responsible for monitoring and protecting Raytheon's intellectual property through legal means and dispute resolution mechanisms.

10. Security Auditing and Assessment Team:
    - Conducts regular security audits and assessments to evaluate the effectiveness of security controls currently in place and to identify areas of improvement.

7.8 Proposed Schedule

Please see Figure 2 on the next page, the proposed 25-week schedule, showing the Raytheon RMP timeline.

7.8.1 Timeline Table

Phase	Steps Involved	Duration
Initiation and Planning	• Define the scope, boundaries, and objectives of the risk assessment. • Identify and appoint a cross-functional risk assessment team consisting of experts from various departments, including cybersecurity, legal, operations, and compliance. • Develop a detailed project plan, outlining roles and responsibilities, and establishing clear communication channels. • Establish the risk assessment budget and secure necessary resources. • Set up regular team meetings and communication mechanisms.	2 Weeks
Asset Identification	• Conduct a comprehensive inventory of tangible and intangible assets, including manufacturing facilities, R&D centers, intellectual property, contracts, financial resources, cybersecurity capabilities, and more. • Document the attributes, values, and criticality of each asset.	2 Weeks

Threat and Vulnerability Identification	• Identify and document threats and vulnerabilities associated with each asset and operation. • Assess external threats (e.g., natural disasters, geopolitical changes) and internal vulnerabilities (e.g., cybersecurity weaknesses, supply chain risks).	2 Weeks
Control Assessment	• Evaluate the effectiveness of existing controls and mitigation measures in place to address identified threats and vulnerabilities. • Determine the adequacy of security measures, and assess their alignment with industry standards and best practices.	3 Weeks
Data Collection	• Collect relevant data on each asset, threat, vulnerability, and control. • Ensure all data is accurate, up-to-date, and consistent across all departments involved in the risk assessment.	3 Weeks
Risk Assessment and Prioritization	• Utilize the collected data to assess the inherent and residual risks associated with each asset and operation. • Prioritize risks based on impact, likelihood, and overall risk ratings. • Use a risk matrix to visualize and communicate the results effectively.	4 Weeks
Documentation and Reporting	• Create a detailed risk assessment report that includes risk profiles for each asset, identified threats and vulnerabilities, control effectiveness, and prioritized risks. • Share the findings with the executive leadership team and other relevant stakeholders.	2 Weeks
Risk Mitigation Planning	• Develop detailed risk mitigation strategies and action plans for high-priority risks. • Define key performance indicators (KPIs) to track progress in implementing mitigation measures.	2 Weeks
Implementation and Monitoring	• Execute the risk mitigation plans according to the established action items and timelines. • Continuously monitor the progress of mitigation measures. • Ensure that controls are functioning as intended and that the organization's risk posture is improving.	4 Weeks

Review and Adaptation	• Conduct a final review of the entire risk assessment process, including assets, threats, vulnerabilities, controls, and mitigation measures. • Identify any lessons learned or areas for improvement. • Use the results to adapt and refine the risk assessment plan for future cycles.	1 Week

Figure 2

8. Risk Mitigation Plan

8.1 Introduction

This risk mitigation plan serves as a strategic roadmap for addressing risks identified in the recent risk assessment. It aims to build upon the insights gained during the assessment phase and provide actionable measures to mitigate potential threats. By implementing these strategies, Raytheon seeks to fortify its position in the military contracting domain. Additionally, the plan serves as a proactive tool, anticipating challenges and offering a dynamic response that goes beyond risk recognition, actively shaping the company's resilience and competitiveness in the ever-evolving landscape of military contracting.

8.2 Scope

This risk mitigation plan covers a wide range of risks associated with Raytheon’s military contracting operations. Not only does it encompass Raytheon’s data center assets and activities, but it also extends to other areas. These areas include production and supply chain, research and development, logistics, and intangible assets such as intellectual property (IP), contracts, and client relationships. This extensive scope

ensures that no crucial act of our organization's business is overlooked when assessing risks.

8.3 Boundaries

The boundaries of this risk mitigation plan focus on tasks directly related to Raytheon's military contracting operations. Any risks that fall outside of this context, such as those associated with a non-military business classification, will not be included. These boundaries are set so that the assessment remains aligned with Raytheon's primary mission, which is to create, innovate, and provide defensive solutions.

8.4 Risk Mitigation Strategies

Please see Figure 3 below addressing risk mitigation strategies based on asset type, asset, and threat type.

Asset - Asset Type	Threat	Mitigation Strategy
Manufacturing Facilities - Hardware (Tangible)	Operational Risk	To address the risks associated with operational disruptions, a comprehensive disaster recovery plan will be implemented. This plan will outline protocols for response and recovery in the event of natural disasters, accidents, or equipment failures. Regular equipment maintenance schedules will also be established to minimize the likelihood of unplanned downtime.
Research and Development (R&D) Centers -	Intellectual Property (IP) Risk	To safeguard intellectual property, access controls will be strengthened, ensuring that only authorized personnel have access to sensitive R&D data. Encryption measures will be

Hardware (Tangible)		enhanced, and regular security audits will be conducted to detect and prevent any unauthorized access or data compromise.
Skilled Workforce - Human Resources (Tangible)	Talent Retention Risk	To mitigate the risk of losing key personnel, Raytheon will offer competitive compensation packages, provide ample professional development opportunities, and foster a supportive work environment. Employee engagement programs will be implemented to enhance job satisfaction and loyalty.
Information Systems - Software (Tangible)	Cybersecurity Risk	To mitigate the risk of losing key personnel, Raytheon will offer competitive compensation packages, provide ample professional development opportunities, and foster a supportive work environment. Employee engagement programs will be implemented to enhance job satisfaction and loyalty.
Supply Chain - Hardware (Tangible)	Supply Chain Disruption Risk	Recognizing the geopolitical and logistical challenges in the supply chain, Raytheon will diversify its suppliers and develop contingency plans. This will ensure a resilient and adaptable supply chain, capable of responding to unexpected disruptions.
Logistics Infrastructure -	Logistics Disruption Risk	To address potential disruptions in logistics, Raytheon will implement route diversification, enhance transport security measures, and establish robust contingency plans. These

Hardware (Tangible)		measures will minimize the impact of transportation issues on product delivery timelines.
Aircraft, Missile, Naval, Satellite, and Land-Based Defense Systems, Electronics and Sensors, Space Technologies, Aircraft Carriers - Hardware (Tangible)	Technology and Product Obsolescence Risk	Recognizing the rapid advancements in technology, Raytheon will invest significantly in research and development for next-generation systems. This proactive approach will ensure that products remain relevant and competitive in the face of evolving technological landscapes.
Data Center - Hardware & Data (Tangible)	Data Center Security Risk	Addressing threats to data center security, Raytheon will implement a multi-layered approach. This includes the deployment of intrusion detection systems, stringent access controls, and comprehensive disaster recovery plans. Regular security audits will be conducted to ensure the ongoing integrity of data center assets.
Defense Technologies - Data (Intangible)	Competitive Risk	To stay ahead in an increasingly competitive landscape, Raytheon will foster a culture of innovation. Continuous research and development efforts, coupled with strategic partnerships, will be the focus to maintain technological leadership.

Intellectual Property - Data (Intangible)	Intellectual Property Infringement Risk	Raytheon will actively monitor patents, seek legal assistance, and employ dispute resolution mechanisms to promptly address any intellectual property infringement claims. This proactive approach will safeguard the organization's intellectual assets.
Contracts and Agreements - Data (Intangible)	Contractual Risk	Raytheon will develop robust contractual agreements that outline security requirements for contractors and business partners. Additionally, the organization will stay vigilant about changes in government procurement policies, ensuring adaptability to evolving regulatory landscapes.
Financial Resources – Data (Intangible)	Financial Market Risk	In response to financial market risks, Raytheon will diversify investments and maintain a disciplined fiscal approach. By closely monitoring economic indicators, the organization will be prepared to navigate potential downturns and market volatility.
Cybersecurity Capabilities - Software (Intangible)	Cybersecurity Risk	Raytheon will conduct regular penetration testing, provide ongoing cybersecurity training for employees, and proactively monitor emerging threats. This comprehensive approach will fortify the organization against potential data breaches and cyberattacks.
Global Network of Clients - Data (Intangible)	Geopolitical Risk	To address geopolitical risks impacting client relationships, Raytheon will diversify its client base and actively manage international relationships. This proactive approach will

		minimize the impact of changes in international relations on business operations.
Data Center - Hardware & Data (Intangible)	Data Center Operations Risk	To mitigate risks associated with data center operations, Raytheon will implement redundancy measures, conduct capacity planning, and establish robust incident response plans. These measures will ensure the continuous availability and reliability of data center operations.

Figure 3

8.5 Controls and Policies

As outlined in the risk assessment, Raytheon will be implementing various controls and policies to mitigate the identified risks. Raytheon's controls include cybersecurity measures, disaster recovery plans, intellectual property protection strategies, supply chain management practices, and compliance measures.

8.5.1 Security Control and Policy List

Security controls and policies Raytheon will be implementing:

1. **Access Control Policies**
    - Implement role-based access control (RBAC) to assign proper permissions based on job roles and responsibilities.
    - Utilize multi-factor authentication (MFA) for additional user verification.
    - *NIST Implementation Method: Procedural Control*
2. **Network Security**

- Implement firewalls and intrusion detection/prevention technologies to protect against unauthorized access and cybersecurity threats.
- Regularly update and patch all network devices and access points to prevent vulnerabilities.
- *NIST Implementation Method: Technical Control*

3. **Data Encryption**
    - Encrypt all data at rest and in transit to prevent sensitive information or intellectual property leaks.
    - Use strong encryption protocols, such as AES (advanced encryption standard), for communication channels and data storage systems.
    - *NIST Implementation Method: Technical Control*
4. **Physical Security**
    - Secure physical facilities, data centers, and manufacturing facilities with access controls, surveillance systems, and intrusion alarms.
    - Implement visitor access policies to control entry to protected areas.
    - *NIST Implementation Method: Physical Control*
5. **Secure Software Development**
    - Implement secure coding practices into the software development workspaces to prevent vulnerabilities in applications.
    - Conduct regular code reviews and software testing.
    - *NIST Implementation Method: Procedural Control, Technical Control*
6. **Security Monitoring and Logging**
    - Maintain comprehensive logs of all network and system activities.

- Implement a Security Information and Event Management (SIEM) system to monitor traffic and detect security incidents.
- *NIST Implementation Method: Technical Control*

7. **Endpoint Security**
    - Use endpoint protection software to secure workstations and mobile devices.
    - Enforce device encryption policies for mobile devices.
    - *NIST Implementation Method: Technical Control*
8. **Contractual and Legal Protection**
    - Develop contractual agreements that outline security requirements for contractors and business partners.
    - Ensure compliance with legal regulations and standards applicable to the military contracting sector.
    - *NIST Implementation Method: Procedural Control*
9. **Security Audits and Assessments**
    - Conduct regular security audits and assessments to evaluate the effectiveness of security controls in place and identify areas of improvement.
    - *NIST Implementation Method: Procedural Control*
10. **Data Loss Prevention (DLP)**
    - Deploy solutions to monitor and prevent unauthorized data transfers or leaks.
    - Implement regular cloud data backups and comprehensive tools for preventing data loss.
    - *NIST Implementation Method: Technical Control*

8.6 Monitoring and Evaluation

Effectively monitoring and evaluating the implemented risk mitigation strategies are crucial aspects of ensuring the ongoing success and adaptability of Raytheon's military contracting operations. This section outlines the key components of the monitoring and evaluation process, including the establishment of Key Performance Indicators (KPIs) and a continuous improvement framework.

8.6.1 Key Performance Indicators (KPI)

To gauge the effectiveness of the risk mitigation strategies, Raytheon will establish Key Performance Indicators (KPIs) that align with organizational goals and objectives. These KPIs will serve as measurable indicators of progress and success. It is essential to regularly review and update these KPIs to ensure their relevance and alignment with evolving risk landscapes.

8.6.1.1 KPI Table: Objectives and Measurements

Please see Figure 4 below referencing established KPIs:

KPI	Objective	Measurement
Incident Response Time	Ensure quick response to security incidents.	Average time taken to respond and contain security incidents.
Cybersecurity Preparedness	Evaluate the organization’s overall cybersecurity readiness.	Regular assessment and simulations of cybersecurity response capabilities.
Supply Chain Resilience	Assess the resilience of the supply chain.	Time taken to recover from supply chain disruptions and the overall adaptability of the supply chain.

Data Center Availability	Ensure continuous availability of data center assets.	Percentage of uptime for critical data center infrastructure.
Employee Awareness	Enhance employee awareness of cybersecurity best practices.	Results from periodic cybersecurity training assessments and simulated phishing exercise.
Contractual Compliance	Ensure compliance with contractual security requirements.	Regular audits to verify adherence to security clauses in contracts.

Figure 4

8.6.2 Continuous Improvement Plan

Continuous improvement is integral to the success of the risk mitigation plan. Raytheon will establish a structured framework for ongoing assessment and refinement of strategies, allowing the organization to adapt to emerging threats and challenges.

8.6.2.1 Four Points of Continuous Improvement

The four points of continuous improvement within Raytheon includes:

1. Periodic Review: Conduct regular reviews of the overall risk mitigation plan, including assets, threats, vulnerabilities, controls, and mitigation measures. Identify any lessons learned, success stories, or areas for improvement.
2. Lessons Learned: Document and analyze incidents, successes, and failures. Utilize lessons learned to refine and enhance risk mitigation strategies.
3. Adaptation: Use the results of reviews and lessons learned to adapt and refine the risk mitigation plan for future cycles. Stay informed about industry best practices and emerging risks to continually improve strategies.
4. Stakeholder Feedback: Gather feedback from key stakeholders, including security teams, executives, and employees. Incorporate constructive feedback into the continuous improvement process.

8.6.3 Reporting Mechanisms

Transparent and regular reporting is essential for keeping stakeholders informed about the progress and effectiveness of the risk mitigation plan. Reporting mechanisms will include:

1. Executive Summary Reports: These are periodic executive summaries outline the overall status of risk mitigation efforts. They highlight key achievements, challenges, and areas for improvement.

2. Detailed Risk Assessment Reports: Includes in-depth reports detailing risk profiles for each asset, identified threats and vulnerabilities, control effectiveness, and prioritized risks. Also shared with the executive leadership team and relevant stakeholders.

3. Incident Reports: Includes detailed reports on any security incidents, outlining the incident response process, lessons learned, and actions taken to prevent future occurrences. These are shared with the incident response team, executives, and relevant stakeholders.

8.6.4 Vulnerability & Exploit Assessment Strategies

Vulnerability and exploit assessment strategies are integral components of Raytheon's broader risk mitigation plan, ensuring a proactive and comprehensive approach to identifying, analyzing, and addressing potential threats and vulnerabilities. Please see the two lists below relating to these strategies.

8.6.4.1 Vulnerability Assessment Strategies List

1. Internal Assessments:

- Description: Evaluate vulnerabilities within the organization by exploiting internal systems.
- Testing/Evaluation Strategy: Security professionals conduct controlled internal assessments to identify weaknesses in servers, networks, and personnel.

2. External Assessments:

- Description: Evaluate vulnerabilities by simulating external attacks from outside the organization.
- Testing/Evaluation Strategy: External personnel attempt to exploit systems to identify vulnerabilities. This provides a perspective on potential threats from external sources.

3. Documentation Review:

- Description: Review documentation, system logs, and audit trails to identify vulnerabilities.
- Testing/Evaluation Strategy: Conduct thorough reviews of incident documentation, past assessment reports, and logs to identify common problems and potential vulnerabilities.

4. Vulnerability Scans:

- Description: Use automated tools to scan systems and networks for vulnerabilities.
- Testing/Evaluation Strategy: Regularly perform vulnerability scans to identify and quantify vulnerabilities. Document the results and use them for further analysis.

5. Audits and Personnel Interviews:

- Description: Conduct audits to check compliance with rules and guidelines, including internal policies.
- Testing/Evaluation Strategy: Perform manual or automated audits to ensure compliance. Conduct personnel interviews to gather additional insights and verify adherence to policies.

6. Process and Output Analysis:

- Description: Analyze firewall rules and outputs to identify vulnerabilities.
- Testing/Evaluation Strategy: Utilize process analysis for systems with fewer rules and output analysis for systems with a higher number of rules. This helps in understanding and mitigating vulnerabilities.

7. System Testing:

- Description: Verify the functionality of systems, access controls, and security countermeasures.
- Testing/Evaluation Strategy: Perform functionality testing, access controls testing, penetration testing, and transaction/application testing to identify and address vulnerabilities.

8.6.4.2 Exploit Assessment Strategies List

1. Simulated Attacks:

- Description: Simulate attacks to determine if vulnerabilities can be exploited.
- Testing/Evaluation Strategy: Begin with a vulnerability test to identify weaknesses and then attempt to exploit these vulnerabilities. This helps in understanding the potential impact of successful attacks.

2. Gap Analysis and Remediation:

- Description: Identify and mitigate exploits by conducting a gap analysis.
- Testing/Evaluation Strategy: Determine which exploits are mitigated and which are not. Use this information to generate a gap analysis report and develop a remediation plan.

3. Configuration or Change Management:

- Description: Implement standards to prevent or remediate exploits by managing system configurations.

- Testing/Evaluation Strategy: Regularly assess and verify that systems are configured according to standards. Implement change management processes to control modifications.

4. Verification and Validation:

- Description: Verify that exploits have been mitigated by retesting vulnerabilities.
- Testing/Evaluation Strategy: After identifying and mitigating exploits, conduct vulnerability scans again, and repeat relevant audits to confirm that the vulnerabilities have been effectively addressed.

5. Best Practices:

- Description: Follow best practices for exploit assessments within the IT infrastructure.

Testing/Evaluation Strategy: Seek permission before conducting assessments, identify as many exploits as possible, use a gap analysis for legal compliance, and verify that exploits have been mitigated effectively.

8.7 Conclusion

In essence, the Raytheon Risk Mitigation Plan is a carefully mapped strategy to deal with known risks in the military contracting sector, drawing insights from the earlier risk assessment. Covering a wide range of assets, both physical and non-physical, and different aspects of operations, the plan closely follows Raytheon's main goal of creating innovative defense solutions. The strategies to minimize risks, such as plans for handling disasters and protecting intellectual property, are tailored to deal with specific threats, ensuring a strong and layered approach to risk management.

The plan's effectiveness is supported by clear roles, a well-organized schedule for risk reduction, and a commitment to continually watch and evaluate the situation. Key Performance Indicators (KPIs) are used as measurable goals, providing clear standards for success. The ongoing improvement plan ensures that Raytheon can adjust to new risks. This active and forward-thinking method not only reduces risks but also positions Raytheon to succeed in the changing world of military contracting, showing a dedication to resilience, innovation, and long-term success.

9. BIA & BCP Plan

9.1 Introduction

The Business Impact Analysis (BIA) and Business Continuity Plan (BCP) for Raytheon have been developed to identify critical business functions, assess potential risks, and establish strategies for business continuity. This approach addresses challenges and disruptions that stand in the way of Raytheon’s commitment to military contracting.

9.2 Business Impact Analysis (BIA)

In this section, the goal is to identify and prioritize the critical business functions of Raytheon. Any essential processes, systems, and activities integral to Raytheon’s success will be included. By recognizing and categorizing critical business functions, the BIA will create a foundation for an effective business continuity plan (BCP).

9.2.1 Critical Business Functions (CBF)

Below is a list of Raytheon’s CBFs:

1. Manufacturing Facilities
2. Research and Development (R&D) Centers

3. Skilled Workforce
4. Information Systems
5. Supply Chain
6. Logistics Infrastructure
7. Defense Technologies
8. Data Centers
9. Global Network of Clients

By identifying critical business functions, vital resources necessary for these functions can also be identified. From tangible assets such as manufacturing facilities, to intangible assets such as intellectual property, the BIA maps out the key resources that must be protected to maintain operational success.

9.2.2 Critical Resources (CR)

Below is a list of Raytheon's CRs:

1. Internet access
2. Cloud/backup storage
3. Network connectivity
4. Database servers
5. Desktop computers

9.3 Maximum Acceptable Outage (MAO) and Impact

This section introduces the concept of Maximum Acceptable Outage (MAO), providing standards for the allowable downtime for each critical business function. Alongside MAO, impact level is also assessed. This offers a qualitive measure of the

potential consequences of an outage. This analysis is crucial for prioritizing recovery efforts and allocating resources efficiently. Please see Figure 5 below:

CBF (Critical Business Function)	MAO (Maximum Acceptable Outage)	Impact Level (Low, Medium, High)
Manufacturing Facilities	72 Hours	High
R&D Centers	72 Hours	High
Skilled Workforce	24 Hours	Low
Information Systems	48 Hours	High
Supply Chain	48 Hours	Medium
Logistics Infrastructure	48 Hours	Medium
Defense Technologies	72 Hours	High
Data Center	72 Hours	High
Global Network of Clients	48 Hours	Medium

Figure 5

- **Manufacturing facilities** typically involve complex processes, and a downtime of up to 72 hours allows for response recovery, and resumption of operations.
- **R&D centers** are critical for innovation. Up to 72 hours are allowed for downtime ensuring comprehensive recovery and preservation of intellectual property.
- A **skilled workforce** is vital, the direct impact of employees' unavailability may be lower, but a larger impact can be seen over time. A 24-hour downtime is reasonable for this function.
- **Information systems** are crucial, and a 48-hour downtime provides a window for addressing these issues without compromising critical data and operations.

- A 48-hour downtime for the **supply chain** considers the need for timely responses to disruptions in the logistics and procurement processes.
- **Logistics infrastructure** plays the primary role in timely product delivery. Allowing a 48-hour downtime ensures sufficient time for recovery without causing significant disruptions.
- Given the importance of **defense technologies**, a 72-hour downtime is realistic for thorough recovery and restoration of these functions.
- The **data center** is the central hub for information storage and processing. A 48-hour downtime provides a reasonable timeframe for recovery while minimizing potential data loss.
- Allowing up to 72 hours for downtime in the **global network of clients** will provide flexibility to address potential disruptions in client relationships and international business ventures.

9.4 Recovery Point Objective (RPO) and Recovery Time Objective (RTO)

Recovery point objective (RPO) defines the maximum acceptable data loss, while Recovery Time Objective (RTO) outlines the timeframe within which critical functions must be restored. These objectives are crucial in shaping Raytheon's recovery strategy, ensuring that our enterprise can return to normal operations without compromising data integrity as quickly as possible.

9.5 Business Continuity Plan (BCP)

Raytheon's BCP is designed to keep operations running in the face of potential disruptions, ensuring military defense capabilities and meeting contractual obligations.

The plan encompasses four key phases, Notification/Activation, Recovery, Reconstruction, and Plan Training, Testing, and Exercising.

9.5.1 Notification/Activation Phase

During the Notification/Activation Phase, the Business Continuity Plan (BCP) coordinator declares the initiation of the phase. Following the declaration, the Damage Assessment Team (DAT) is mobilized to assess and report the extent of the damage incurred. The activation protocols are then implemented based on the findings provided by the DAT. For instance, in a scenario of a winter storm, a specific risk assessment for employee travel and the activation of remote work procedures become crucial components of this phase.

9.5.2 Recovery Phase

In the Recovery Phase, the Tactical Response Team (TRT) steps in to restore temporary operations to critical systems. The TRT directs its efforts toward the recovery of the identified Critical Business Functions (CBFs). For instance, in response to a winter storm, the TRT would focus on ensuring the functionality of remote work capabilities, addressing any disruptions caused by weather conditions.

9.5.3 Reconstruction Phase

In the Reconstruction Phase, the emphasis shifts towards bringing both critical and noncritical functions back in place. This involves repairing damage to the original site, and in certain cases, considering the possibilities of permanent relocation. For instance, in the scenario of a winter storm, deactivation of the TRT would occur once the storm has passed, and regular operations would return.

9.5.4 Plan Training, Testing, and Exercising Phase

In the last phase of the business continuity plan, it focuses on the preparations for possible disruptions occurring. The primary goal here is straightforward: ensure everyone knows the BCP inside out.

Training becomes pivotal as informing personnel of the intricacies of the BCP is crucial. The emphasis is on equipping every team member with the essential skills to navigate remote access and utilize Virtual Private Networks (VPNs). This practical knowledge is fundamental to ensuring a seamless transition when the BCP is invoked.

Testing takes the form of stress-testing the BCP under realistic conditions. By subjecting our plan to simulated scenarios, we aim to identify and rectify any vulnerabilities or inefficiencies. The goal is to enhance the robustness of our BCP and strengthen Raytheon in its week points.

Exercises serve as a practical link between theory and real-world application. This approach is straightforward and pragmatic, ensuring personnel not only comprehend the BCP specifics but executes them with precision. Emphasizing practical preparedness, Raytheon's BCP functions as a dynamic tool consistently ready for swift and effective deployment. The approach is rooted in practical readiness, avoiding unnecessary complexities and emphasizing the maintaining of operational resilience without compromising the integrity of the document.

9.6 Cost-Benefit Analysis (CBA)

The Cost-Benefit Analysis (CBA) section provides a financial perspective on the proposed strategies within the BIA and BCP. The costs associated with implementing

recommendations, projected benefits, and a control factor all contribute to the overall CBA.

9.6.1 Cost to Implement Recommendations

Please see the list below outlining the cost to implement recommendations.

1. Training Programs:
    - Cost: Approximately $50,000 for comprehensive employee training programs.
    - Benefit: Improved staff readiness during disruptions, minimizing downtime.
2. Technology Upgrades:
    - Cost: Estimated at $200,000 for investing in updated technologies for enhanced data backup and recovery capabilities.
    - Benefit: Reduced data loss and quicker recovery times.
3. Infrastructure Resilience Enhancements:
    - Cost: Capital investment of around $500,000 in reinforcing critical infrastructure against potential disruptions.
    - Benefit: Increased resilience, minimizing the impact of physical threats.
4. Testing and Simulation Tools:
    - Cost: Approximately $75,000 for the procurement of advanced testing and simulation tools for BCP stress testing.
    - Benefit: Improved identification of vulnerabilities and enhanced plan robustness.

9.6.2 Projected Benefits

Projected benefits within the plan are listed below.

1. Reduced Downtime:

- Implementation of robust BCP measures is projected to save an estimated $1,000,000 annually in reduced downtime during disruptions, leading to increased operational efficiency.

2. Enhanced Data Integrity:
    - Investments in technology upgrades and data recovery capabilities are expected to ensure better data integrity, potentially saving $500,000 per major disruption in terms of prevented data loss.
3. Minimized Financial Losses:
    - By minimizing downtime and ensuring continuity, the organization anticipates a conservative estimate of $2,000,000 in annual reduction in financial losses associated with disruptions.
4. Operational Resilience:
    - Strengthened infrastructure and comprehensive training programs are projected to enhance operational resilience, potentially saving an additional $1,500,000 in avoided operational disruptions.

9.6.3 Control Factor

To assess the overall feasibility and success of the proposed strategies, a control factor will be employed. This involves monitoring and adjusting strategies based on ongoing evaluations, industry best practices, and emerging risks. Regular reviews and adaptations to the BCP will ensure its continued effectiveness and alignment with the evolving risk landscape.

9.6.4 Summary

The Cost-Benefit Analysis demonstrates that while there are initial costs associated with implementing recommended strategies, the projected benefits in terms of reduced downtime, enhanced data integrity, minimized financial losses, and improved operational resilience outweigh the investment.

Total Cost of Implementation:

- Training Programs: $50,000
- Technology Upgrades: $200,000
- Infrastructure Resilience Enhancements: $500,000
- Testing and Simulation Tools: $75,000
- Total Estimated Cost: $825,000

Total Projected Benefits:

- Reduced Downtime: $1 million annually
- Enhanced Data Integrity: $500,000 per major disruption
- Minimized Financial Losses: $2 million annually
- Operational Resilience: $1.5 million in avoided operational disruptions
- Total Estimated Annual Benefits: $5 million

Net Benefit (Annual): $5,000,000 - $825,000 = $4,175,000

The control factor adds a dynamic element, ensuring that the Business Continuity Plan (BCP) remains adaptive and effective in the face of changing circumstances. Raytheon's commitment to innovation and sustained success is further fortified by a

strategic financial perspective embedded in the CBA, with an estimated net annual benefit of $4,175,000.

9.7 Conclusion

In conclusion, the Business Impact Analysis (BIA) and Business Continuity Plan (BCP) for Raytheon are robust frameworks strategically created to support the enterprise's resilience and operational efficiency in the face of the military contracting world. The BIA identifies and prioritizes critical business functions, providing a foundation for the comprehensive BCP. By outlining tangible and intangible crucial resources, Raytheon ensures the safeguarding of assets crucial for sustained success. The establishment of Maximum Acceptable Outage (MAO) times, reflecting realistic downtime limits for each critical function, allows for efficient resource allocation and prioritized recovery efforts.

Furthermore, the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) shape Raytheon's recovery strategy. They emphasize the importance of data integrity and restoration of critical functions. The BCP, structured into Notification/Activation, Recovery, Reconstruction, and Plan Training, Testing, and exercising phases, provides a dynamic and proactive approach to potential disruptions. Each phase reflects the plan's adaptability to diverse challenges.

The Raytheon BIA and BCP represent a comprehensive strategy that aligns with the enterprise's mission in military contracting. By addressing challenges head-on, Raytheon not only backs its operational capabilities but also reaffirms its commitment to innovation, resilience, and sustained success in the ever-evolving landscape of military contracting.

References

[1] Anon. 2021. Ear (Export Administration Regulations) - ear export control. (October 2021). Retrieved October 6, 2023 from https://www.exportsolutionsinc.com/ear/#:~:text=The%20Export%20Administration%20Regulations%20(EAR)%20are%20controlled%20by%20the%20U.S.,could%20also%20have%20military%20applications.

[2] Anon. 2023. Foreign Corrupt Practices Act (FCPA). (June 2023). Retrieved October 6, 2023 from https://www.sec.gov/enforcement/foreign-corrupt-practices-act#:~:text=The%20Foreign%20Corrupt%20Practices%20Act,in%20obtaining%20or%20retaining%20business.

[3] Anon. 2023. What is vendor management?: Definition & process. (September 2023). Retrieved October 6, 2023 from https://taulia.com/glossary/what-is-vendor-management/#:~:text=Vendor%20management%20includes%20activities%20such,risks%20and%20ensuring%20service%20delivery.

[4] Anon. DPC: Defense Acquisition Regulations System: DFARS/PGI. Retrieved October 6, 2023a from https://www.acq.osd.mil/DPAP/dars/dfarspgi/current/index.html#:~:text=Defense%20Federal%20Acquisition%20Regulation%20Supplement,for%20the%20Department%20of%20Defense.

[5] Anon. Federal Acquisition Regulation (FAR). Retrieved October 6, 2023b from https://www.gsa.gov/policy-regulations/regulations/federal-acquisition-regulation.

[6] Anon. Federal Information Security Modernization Act: CISA. Retrieved October 6, 2023 from https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act.

[7] Anon. National Industrial Security Program Oversight. Retrieved October 6, 2023b from https://www.dcsa.mil/Industrial-Security/National-Industrial-Security-Program-Oversight/#:~:text=The%20National%20Industrial%20Security%20Program,or%20research%20and%20development%20efforts.

[8] Juliana De Groot, Conor Roach, and Nate Lord. What is ITAR compliance? (regulations, fines, & more). Retrieved October 6, 2023 from https://www.digitalguardian.com/blog/what-itar-compliance#:~:text=What%20does%20it%20mean%20to,States%20Munitions%20List%20(USML).

[9] Neena Shukla and Neena Shukla. 2022. What you need to know about government contracting laws: Far and beyond. (September 2022). Retrieved October 6, 2023 from https://www.pbmares.com/government-contracting-laws-far-and-beyond/#:~:text=The%20Federal%20Acquisition%20Regulations%2C%20also,well%20as%20any%20related%20rules.