Risk Management Plan

Outline

- **Risk Management Plan**
  - **Purpose and Importance**
  - **Outline**
  - **Scope and Boundaries**
  - **Schedule**
  - **Regulations**
- **Risk Assessment Plan**
  - **Executive Summary**
  - **Scope and Boundaries**
  - **Approaches**
  - **Roles and Responsibilities**
  - **Schedule**
  - **Countermeasures**
  - **Identification of Risks**
- **Risk Mitigation Plan**
  - **Cost**
    - **Initial Costs**
    - **Faculty Costs**
    - **Facility Costs**
    - **Installation Costs**
    - **Training Costs**
  - **Schedule**
  - **Operational Impact**
- **Introduction and Business Impact Analysis Plan**
  - **Purpose and objectives**
  - **Outline**
  - **Critical business functions**
  - **Critical Business Resources**
  - **Business RTOs**
  - **Direct Cost**
  - **Cumulative Dollar Loss Ranges (Tangible)**
  - **Intangible Costs**
  - **Recovery Requirements**
    - **High Level**
    - **Medium Level**

        - **Low Level**
- **Business Continuity Plan**
    - **Purpose**
    - **Scope**
    - **Assumptions and Planning Principles**
    - **Incident to be included and excluded**
    - **Strategy**
    - **Priorities**
    - **System Description and Architecture**
        - **Overviews**
    - **Functional Description**
    - **Sensitivity of Data and Critical of operation**
    - **Telecommunication**
    - **Responsibilities**
    - **Order of Succession and Delegation of Authority**
    - **Notification/ Activation Phase**
    - **Notification Procedures**
    - **Damage Assessment Procedures**
    - **Plan Activation**
    - **Recovery Phase**
    - **Recovery planning**
    - **Recovery Goal**
    - **Reconstitution Phase**
    - **Original or New Site Restoration**
    - **Concurrent Processing**
    - **Plan Deactivation**
    - **Plan training, Testing, and Exercises**
    - **Plan Maintenance**

Purpose and Importance

The purpose of this document is to establish the guidelines and boundaries to the network established by the Defense Logistics Information Service (DLIS). The contents of this document comprise of, but are not limited to; the required procedures based on the Defense Logistics Agency (DLA), the use of policies established by the DLA and their implementation to DLIS, and the guidelines to be maintained upon establishment

of new procedures.

Outline

The basis of the contents of this document is to be provided as a guide to the addition of tasks needed to appropriately manage risks in the company. The main components and methods of accomplishing are:

- **Identification of threats and vulnerabilities**
    - Conduct a survey of the current site and identify what areas of the network are to be worked on.
    - Perform a site survey and build a physical review of the areas of key business operations.
    - The assessed threats would be then categorized into different sections based on the likelihood and cost for replenishing lost resources.
- **Assigning responsibilities**
    - Establish a plan where each department would be taking care of their own responsibilities as needed to maintain, establish, and develop the systems on which they rely on.
- **Mitigation techniques**
    - The teams of key members will establish a list of possible methods to mitigate the vulnerabilities established from the previous surveys of the location as per their professional opinion.

- **Collect CBA information**
    - A separate survey of the stakeholders will take place to realize what are the most necessary applications needed to maintain business productivity at a maximum.
- **Identify costs**
    - A professional opinion of the needed software, hardware, and human resources will be taken and an accurate rough estimate will be established to asses any needed remediation.
- **Document accepted mitigation techniques**
    - The best methods of mitigation of the vulnerabilities identified will be chosen and will be documented as part of the risk management plan for the business.
- **Create a plan of action and milestones**
    - A plan will be developed to list the necessary work packages needed to complete said project and complete major milestones in the allotted times.

Scope and Boundaries

The subject of matter is an addition of systems for the DLIS Company. The range and subject matter of the document is the safe addition of these systems and maintaining accurate DLA standards. The specifics of particular allowed systems are not covered upon, but are limited to following the established regulations of the purposed scope. This document is also establish to protect all of the affected parties of the company and is not limited to the hired employees. All risks are evaluated in a scale of occurrence or

level of effect from Low to High. The establishment of the framework by this document is to be followed by the employer regularly and maintained regularly for consistency and accuracy.

Schedule

- **Approval of the risk management plan**: Assigned to the project manager and is due 1 week after submission.
- **Threat Identification**: Assigned to the head IT security specialist and a full report is due within the next week from assigning the task.
- **Identification of Vulnerabilities**: Assigned to head IT security specialist and is due 2 weeks after the submission of the identification of the threats.
- **Solutions Identification**: Assigned to the IT department of the company and a report of all possible solutions and cost implementations are due 2 weeks from assignation.
- **Solutions Selection**: Assigned to the project manager and is discussed with the company corporate leaders and a selection of solutions is to be selected within 4 days from discussion.
- **Preparation of Risk Management Plan**: Assigned to lead project writer and is to be started immediately from the project acceptance of the management plan and to be updated along all points of the project development. It is due 2 days after final solutions are identified.

Regulations

The following regulations are to be followed and to be consulted upon for the implementation and development of any plan staging:

- DLA
- HIPAA
- SOX
- PCI DSS
- FISMA
- NIST/CobiT

Risk Assessment Plan

Executive Summary

Explained in this risk assessment plan, it will be covered on the types and values of the risks assessed for the work environment. It will also explain the necessary procedures to remediate the assessed risks and categorize them accordingly in a three tier system. The cost of the implementations needed to accurately mitigate said risks. Lastly, establish a guideline to the physical implementations needed to complete the full mitigation process by which this company is to adhere to.

Scope and Boundaries

The assessment area of this plan will be contained within the scope purposed. The scope of which the assessing of risks for the company pertaining to the managing of information as used by the company. This, however, is bounded to the boundary of which anything else that does not directly involve the resources used. For the use of this document the outer boundaries that are set in the internet, while the inner boundaries are to be expressed as the intranet. The networking hardware maintained in both these areas are maintained under this scope as they directly fall under the direct criteria of the security of the information transferred along the network as a whole. Only said software that captures and sends classified or important records of the company that also fall under the DLA guidelines for information, would be considered to be a part of this scope as well. Lastly, all users that directly access the internetworking of the company should fall under the umbrella scope and comply by this plan. All boundaries

are subject to change and are open to addition as new regulation and guidelines are developed.

Approaches

The major forms of identifying and evaluating the relevant threats that affect the company will be found with the following methods:

- Looking into historical data that has been stored in the internal networking systems
    - This is effective to use because all threats that have already affected the systems in place for the company are placed out in these logs.
- System models of the new and older systems
    - By looking at the systems from the attackers perspective all pertinent vulnerabilities are easily scouted out and methodologies are established for the future identification of threats for the system and possible mitigation techniques.
- Penetration tests
    - By forcefully attempting to break into the system the organization can see the possible damages and loss of resources needed to properly assess the threats of the occurring breach.

Roles and Responsibilities

For the development of the risk assessments of the organization certain key personnel and departments will take part for the establishment for this document.

- Contracted/Internal IT Security Specialist
    - Responsible for the assessments for the internal network in relations to the related costs and equipment necessities based on the professional opinion on such tasks.
    - Create and rate the occurrence probability for the said risks to properly evaluate the risks that must be mitigated to those that can be more lenient towards mitigation.
- IT systems Managers
    - Provide information on common system disabilities and curative measures for the occurances.
- IT Department
    - Inform of other common system faults.
- On-Site Security

    - Obtain common procedures and faults of physical security procedures and limitations.
- Project Manager/Site Supervisor
    - Formulate the proper assessment criteria for the information gathered and appropriately prepare for the reporting of the assessed risks for the company and relate to the operational and potential loss of a occurrence of a breach.

Schedule

- Establishment of the Risk Mitigation Plan: Assigned to the project manager and is due 3 days after approval from the higher management officials.
- Begin Site Survey: Assigned to the designated IT securities expert and is due 10 days after the initiation of the said task.
- Create the Possible Mitigation Techniques: Assigned to the IT securities professional and/or the IT Department individuals whom mainly follow that specific criteria or area. This task is due 10 days after the initiation of the necessary business meeting for the IT staff to converse about said topic.
- Selection of Mitigation Techniques: Assigned to the project manager and is due within the next 3 days after accepted methods selected by the higher management officials from the company.
- Begin Mitigation Plan: Assigned to all IT staff implementing the physical and logical network, as well as all security staff that handles all internal business physical countermeasures. The full implementation and testing of said event is due within 60 to 90 days of the start of the build.

Countermeasures

Countermeasures are the methods that were identified to be the best method into mitigating the risks that were opposing the DLIS company. Some of these countermeasures are in-place countermeasures where they use the current systems in place for the company, and simply enhance their current abilities to comply with the risk mitigation request. As the countermeasures are processed some may already be a planned countermeasure already, were they have a schedule in place for the steps needed to complete the major tasks for the countermeasure. Some countermeasures may just be at the approval stage where they have been approved, but have no set schedule. Some may be very complex procedures that are just documented as the necessary steps are taken to complete the final project.

Identification of Risks

In order to identify the risks associated to this company, all relevant aspects within the scope of the project must be examined to recognise any relevant threats that may occur, or breaches that have occurred. After finding out any weak entry points a list of the risks alongside their associated risk counterparts will be established for the necessary countermeasures that are needed to prevent any breaches in the confidentiality, integrity or availability of the company.

Risk Mitigation Plan

The risk mitigation plan will detail the risks and associate the cost and the benefit in relation to the cost to numerically measure out the relation from the cost to the benefit of implementing the mentioned mitigation techniques.

Cost

The cost of the implementation will be separated based on initial, one time, costs; employee hourly wages; facility upkeep costs; one time installation fees; and training costs per training session.

Initial Costs

Costs from the implementation that are up-front fees for the use of the mitigation technique. For example, the purchase of a $10,000 firewall to protect the network from outside port finders. These costs do not repeat unless multiple units are purchased for the use of the company. In which case should be totaled and given a per item price overview.

Faculty Costs

Faculty costs are referred to hourly, daily, weekly, etc. payments that are set to the labour for the employee workforce maintaining and monitoring the set implementation techniques. The costs of individual contractors and experts should be included as well.

Facility Costs

The amount of money it takes to maintain the location for the specified implementation. For example, maintaining a server rack with multiple switches and virtualized servers

may take a constant cool stream of air passing through the components to prevent overheating and the cost to keep both the conditioning unit and servers running. Some components as well require multiple failovers that also require other costs, such as a UPS.

Installation Costs

The cost associated with having professional installation to the actual location. Some implementations may not require any installation at all, while others require a revamp of the entire company's warehouse structure. An example of such an occurrence is the new installation of a fire system where all rooms in the building must have a fire shower head and automatic power lock in the case of an outbreak.

Training Costs

These are the individual costs necessary for the training of current workforce employees to the use of any new system implemented to the company. Some systems require large training sessions where not only does it require a large amount of revenue, it also requires the employee to spend multiple hours to become proficient on the systems.

Schedule

- **Obtain authorization** - assigned to the project manager and is due within 1 week from assignation
- **Identification of the countermeasures** - Assigned to the assigned expert and is due within 2 weeks from assignation
- **Any relevant countermeasure time arrangements** - Assigned to the assigned expert and is due with the identification of the countermeasures
- **Cost analysis in relevance to the identified countermeasures** - Assigned to the project manager or accounting executive and is due within 3 weeks from assignation
- **Obtain secondary approval based on cost** - Assigned to the project manager and is due 3 days from assignation.
- **Schedule creation of the individual tasks for the project** - Assigned to the project manager and is to be regularly updated until the end of the project, it is to be created immediately from the finishing of the cost analysis
- **Obtain final approval of the appropriate countermeasures** - Assigned to the project manager and is due within 3 days from assignation

Operational Impact

In order to maintain great security some tools may be implemented to the organization that may be more difficult than the previous systems'. In order to prevent the loss of business function, the employees directly using these systems need to be trained and familiar to the use and steps to accomplish the needed tasks to maintain a secure and accurate workflow. This may cause a initial cost for the business, but inturn save the business both productivity and integrity in the long run.

Introduction and Business Impact Analysis

Purpose and objectives

The purpose of the business impact analysis (BIA) is to identify the impact of the outages on the business in direct relation to the critical business functions (CBF) and which business units/departments and processes are critical to the success of DLIS organization. The BIA will identify how quickly essential business units and/or processes have to return to full operation following a disaster situation. A business impact analysis is done to determine which tasks and functions are critical for the foundation to stay in business. The foundation and its business groups must determine what is required for survival of the organization. It is also in this plan to maintain the business' critical success factors (CSF) in relation to identifying the maximum allowable outage (MAO) times.

The objectives of the BIA are as follows:

- Estimate the financial impacts for each business unit.
- Estimate the intangible (operational) impacts for each business unit.
- Identify the organization's business unit processes and the estimated

recovery time frame for each business unit.

Outline

Each Facility Business Continuity Planner (FBCP) or accounted for expert, shall perform a BIA on all business processes to determine the criticality of these processes to DLIS and to determine what the impacts are to the organization if those processes were interrupted. It shall identify the business process availability and the related Recovery Time Objectives (RTOs), and the business process Recovery Point Objectives (RPOs) for all key business processes.

Critical business functions

Below are the main CBFs that are essential to maintain for said business:

- Customers accessing the web site
- Web server accessing the database server
- The order-processing application receiving and processing the order

Critical Business Resources

These resources are essential to maintaining all CBFs and must be available in the case of a disaster. Below are a few listed functions that are necessary to maintaining these CBFs:

- Network Connectivity
- Warehousing Application

- Employee Availability
- Database Server

Business RTOs

The business' RTO are based on the criticality on the systems and functions that serve the direct or indirect revenue. The criticality of these systems and functions will be separated by implementing levels of criticality as stated below:

Value level	MAO	Activity	Impact
Level 1	2 hrs	Available all business hours	Outage will have immediate impact on business
Level 2	1 day	Business processes can survive for a short time	Outage will have a medium impact with no large revenue loss
Level 3	7 days or more	Business processes can survive for 7 days or longer	Outage will have little to no impact on the business

Direct Cost

The direct costs associated to the loss of a CBF are tangible monetary loss values that affects the organization. The following number score have been established to provide firm tangible categorizations for the organization in relations to the monetary loss.

Cumulative Dollar Loss Ranges (Tangible)

Score	Loss Range
0	none
1	< $3,000
2	≥ $3,000 < $10,000

3	≥ $10,000 < $15,000
4	≥ $15,000 < $20,000
5	≥ $20,000 < $40,000
6	≥ $40,000 < $80,000
7	≥ $80,000 < $150,000
8	≥ $150,000 < $250,000
9	≥ $250,000 < $500,000
10	≥ $500,000

Intangible Costs

Such costs are referred to any loss to the business that is not directly related to revenue, however affects the business in a secondary form. Such intangible costs consist and are not limited to:

- Loss of trust from the consumers
- Loss of trust with other businesses
- Loss of employee morale
- Lost opportunities during recovery

Recovery Requirements

By the use of the levels stated below, services and systems will be categorized to effectively address the severity and necessity to addressing any unavailability to these systems or services. Two primary terms related to the recovery requirements are (RTO) recovery time objectives and (RPO) recovery point objectives.

RTO: (applies to all system/function) is the time in which the system/function must be recovered

RPO: the maximum amount of data loss a DLIS organization can accept.

High Level

Immediate restoration required. Maximum outage/downtime is between one and five days before the foundation suffers severe legal, reputational or financial impact.

Medium Level

Function can continue in default mode or not performed for two to four weeks.

Immediate restoration not required. Failure to perform these will eventually impact performance of high level functions, but will not result in severe legal, reputational or financial impact.

Low Level

Function can continue in default mode and not performed for extensive amounts of time. Function can be delayed until operating environment has been restored to normal.

Business Continuity Plan (BCP)

Purpose

The BCP will help the organization plan for a major disruption or disaster and ensure that critical business functions (CBF) continue to operate. The goal is a continuation of all, if not most, major operations and to restore services to the most possible extent. All organizational sites are expected to implement the preventive measures stated in the BCP whenever possible to minimize operational disruptions and to recover as rapidly as possible when an incident occurs.

Scope

The scope of the BCP is a global view of the organization. It includes the IT systems, the facilities, and the personnel. The BCP identifies the elements that are mission critical and need to continue to operate. Mission critical are any systems identified as critical to the organization and also apply to function and processes.

Assumptions and Planning Principles

This includes the incidents plan to address in the organization's plan. Also included elements such as strategy, priorities, and required support. The key planning principle is the length of time we expect to continue operations under the BCP before returning to

normal operations.

Incident to be included and excluded

These are the incidents found to be possible due to the variables associated to the organization. It is made up of possible: location, hardware, software, and natural faults that may occur.

- Snow storm, flood, and fire.
    - Flood: Inflatable boats with motor and paddles
    - Seven days of supplies (generator, fuel, food and water)
    - Fire extinguisher
- Power loss
    - Backup generator (7 days fuel)
- Air condition system and heating
    - Cooling system backup
- Earthquake
    - Know proper procedures to stay in cover
    - Drills
    - Seven days of supplies (generator, fuel, food and water)
- **Excluded:** Nuclear War, Hurricane, Tornado

Strategy

(May be changed to accommodate locational factors from other locations, if not listed)

- Location
    - DLIS headquarters data center
    - Warm site (50 miles away)
        - Redundancy backup
        - Redundancy backup for all resources
- Transportation
    - 4x4 emergency vehicle (evacuation)
    - Inflatable motor boat (flood)
- Notification
    - BCP manager notifies senior management and BCP coordinator with procedures
    - BCP coordinator notifies team leads with procedures
    - BCP team leads notifies the teams with procedures
- IT Systems

        - Redundancy backup for all resources
            - 50 File Servers
            - 12 Database
            - Network redundancy (redundant topology)
- Supplies
    - Equipments supplies for BCP to be back on operation
- Utilities
    - Water, food, power, and gas for at least 7 days
- Communication
    - Company push to talk phones

Priorities

Below are listed CBFs, critical resources, and listed in order from most important to least

- Employee safety
- Web Server
- Database Server
- Transaction Applications

Required Support:

- Senior Management full support and approved all funds
- BCP Manager

System Description and Architecture

This section will overview the major components that need to remain operational during a disruption

Overviews

Headquarter database synchronizes with warm site

Headquarter network redundancy with warm site

Functional Description

Servers includes fault-tolerant capabilities with clusters that allow one server to fail without affecting the service provided by the database. Servers also include a redundant array of independent disks (RAID) configurations. RAID drives can fail but

the system will continue to operate, and allow for faster backups.

- DLIS Headquarters
  50 file servers, 12 database servers, Router, Switches, Modem, Web server, Firewalls
- Warm sites/ remote office
  File servers, database servers, Switches, Modem(s), Web server, Firewalls

Sensitivity of Data and Critical of operation

All systems are synchronized with warm site/remote office

- Network Redundancy
- File server redundancy
- Database server redundancy

Critical Equipment, Software, Documents, and Supplies are also needed to be readily available and must be properly documented to ensure availability and function.

Telecommunication

External connection via internet service provider (ISP) dedicated to WAN lines and also Virtual Private Network (VPN). Also alternate Link via modem.

Responsibilities

BCP Program Manager: Manages multiple BCP projects, ensures that BCP is progressing as expected and is activated in a timely matter.

BCP Coordinator: In charge of a specific BCP weather the developing and completing the BCP. Also responsible for declaring the emergency and activating the BCP.

Emergency Management Team (EMT): Senior Managers, direct authority for the recovery of the system.

Damage Assessment Team (DAT): Assesses the damage and declares the severity of the incident.

Technical Recovery Team (TRT): Responsible for recovering the critical IT functions.

Key Personnel

- Critical vendors - Supply the organization with the needed items to maintain product availability.

- Critical contractor - Contracted employees that are experts in the field they represent, essential to restoring some CBFs.

Order of Succession and Delegation of Authority

- CEO
- CIO
- VPs
- Department Directors
- Senior Managements
- BCP Project Manager
- BCP Coordinator
- BCP Lead/Teams

Notification/ Activation Phase

This is done by the BCP Coordinator and should be done when disaster is imminent. The amount of time to accurately notify personnel and management of a disaster should be prompt and the actions in relation to the timeframe should accompany the strategies mentioned above.

Notification Procedures

Notify BCP Coordinator of any disruption or disaster covered by the BCP. Phone in direct hierarchy tree to notify the teams and team members. I.E. BCP Coordinator notifies the team leads for the EMT, DAT, and TRT. Team leads notify all the member of the teams.

Damage Assessment Procedures

The damage assessment team (DAT) is responsible for assessing the damage and reporting the damage to the BCP coordinator. Team's primary goal is to identify the extent of damage as quickly as possible. Reports are then passed to the EMT lead and BCP coordinator to determine on what steps to take.

Plan Activation

Valid reason to activate the BCP

- Safety of personnel
- Damage to the building affecting critical business function
- Loss of operations of one or more critical business function
- Natural disaster strike from weather forecast

Recovery Phase

TRT members are to use specific DRPs to recover individual systems.

Main Goal

- Restore temporary operations to critical systems.
- Repair damage done to original systems.
- Recover damage to original systems.

Recovery planning

DRP will identify the steps and procedures to restore and recover systems after an incident.

Recovery Goal

The DRP guides the work, but it is possible that the work will be in phases, depending on the depth of the recovery.

Technical Recovery Team Lead

TRT lead will oversee the work done by the TRT.

Technical Recovery Team

TRT performs the recovery work.

Reconstitution Phase

Return to normal operations. This includes both the critical functions and the non-mission- essential functions.

Original or New Site Restoration

If the damage to the original location is extensive and the management decides to move. The move will have many factors.

Concurrent Processing

Operations running at two separate locations at the same time. Instead of moving over

completely, you can run operation on both sites at the same time. The main goal is to keep the alternate location up and operational until it is sure the original location is operational.

Plan Deactivation

Deactivate the BCP once everything is normalized. Need necessary clean up to how it was before the disruption.

Plan training, Testing, and Exercises

BCP Training

Teach people details about the BCP. Training should be conducted at least once a year.

- Training session for all teams
    - This give everyone an overall idea of the plan, and how each one fits into its success.
- EMT training
    - This training is targeted at members of the EMT. It identifies their specific responsibilities.
- DAT training
    - this training target he member of the DAT. It stresses the importance of the assessment and identifies tools and checklists to use.
- TRT training
    - This training target the member of TRT. It includes reviews of each of theT individual disaster recovery plans.

BCP Testing

Show that the BCP will work as plan. Testing will be done at least once a year. Testing should reveal any problems or deficiencies with the plan.

BCP Test Exercises

Show how the BCP will work. BCP exercises should be challenging but realistic and problems should be solvable..

Tabletop Exercises

An exercise that brings all the team members together to talk through the process. The BCP coordinator presents a scenario to the team and the team members identify what to-do to respond to the scenario.

Functional Exercises

A functional exercise evaluates specific functions within the BCP.

Full-scale Exercises

Simulate an actual disruption of critical business functions. Full-scale exercises required many resources to complete. Full-scale exercises provide the most realistic view of how team member will respond to an actual emergency.

Plan Maintenance

BCP coordinator is responsible for the BCP plan. This includes reviews and updates of the BCP.

BCP Plan Revisions Tracking

All revisions to the BCP are needed to be documented and maintained by the BCP coordinator.

BCP updates based on changes within the IT infrastructure

Review the BCP when any substantial changes occur within the IT infrastructure.

BCP testing

This review ensures that all the issues identified in the training, testing, and exercises.