Mission BCP and DRP Checklist

A Mandatory Reference for ADS Chapter 545

New Reference: 06/05/2006
Responsible Office: M/DCIO
File Name: 545mbi_060506_cd44

Information System Security
Mission Business Continuity Planning and Disaster Recovery Checklist

for Executive Officers, Information System Security Officers and System Managers

1. Introduction

The General Support System, AIDNET, includes the network infrastructure at USAID/W and the Missions; its critical assets, deployed at the Missions, are controlled from USAID/W. Since your Mission network is an extension of AIDNET, it does not require a separate Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP).

However, risk identification and mitigation are important at your Mission. Risk is your exposure to Mission service outage or interruption. By conducting a risk assessment, you can determine the threats to your Mission that could disrupt its services. After determining and understanding these risks, you will be able to plan for and provide adequate and cost-effective controls and safeguards to protect your Mission's services.

The adequacy and cost-effectiveness of your chosen risk controls, beyond those that are required, are subjective. Given the distributed nature of USAID, as long as you can recover your Missions services elsewhere (to include USAID/W), you can meet your goals for business continuity and disaster recovery. Controls that you can consider may include: 1) shipping copies of your data off-site monthly, 2) adding hardware and bandwidth to "mirror" your services at another Mission or USAID/W, or 3) having a local cold or warm site where you can recover. Your selection of control depends upon your cost, reliability, and time-to-recover requirements.

You should be able to complete a basic risk assessment in several hours. For the risks you identify, you will be able to determine appropriate security controls to mitigate or eliminate the risk, or determine whether you can accept the residual risk.

2. Risk Assessment

There are three basic types of threat: natural (acts caused by nature), manmade (acts caused by man) and environmental (acts related to your Mission's technology). Several examples of each threat type are listed in the table below. It contains several other fields, specifically likelihood, impact, risk level, and a column for whether or not there is a warning for the identified threat.

- **Likelihood** – What is the likelihood that this particular threat will actually occur at your Mission? For Not Applicable use 0, Low use the value 0.1, for Medium use 0.5, for High use 1.
- **Impact** – What is the impact from this particular threat to your Mission? For Low use the value 10, for Medium use 50, for High use 100.
- **Risk Level** –This value is calculated by multiplying the Likelihood value by the Impact value. However, you may adjust it subjectively to better state your understanding of the impact to the Mission.
- **Warning/No Warning** – Will you have advanced warning that the threat will occur (a time-period during which you can take preventative or mitigating actions)?

The following threats within the table are common ones for your consideration. The list is not exhaustive, and you should identify threats that are specific to your Mission environment. If you require assistance with determining likelihood, impact or risk level, send e-mail to the **ISSO@usaid.gov**. The first few threats values are pre-populated as examples.

Threat	Likelihood	Impact	Risk Level	Warning/ No Warning
Natural				
Earthquake	0.5	100	50	
Fire	1	100	100	
Flood	0	10	0	
Storm	0.5	50	25	
Manmade				
Arson				
Civil Unrest				
Sabotage				
Terrorism				
Theft				
Environmental (Non-Data)				
Air Conditioning Failure				
Electrical Power Failure				
Equipment Failure				
Telecommunications Service Failure				
Environmental (Data)				
Record or Data Loss				
Disclosure of Information				
Mission-Specific Threats				

This table contains some example threats likelihood, impacts, risk level, warning type.

3. Impact Analysis

You can now prioritize the threats based upon their Risk Level scores. Where possible, you should select controls or mitigating factors for the threats with the highest Risk Level scores first.

4. Preventative Controls and Mitigating Action

The following controls and mitigating actions within the table are common ones for your consideration for the previously identified threats. The list is not exhaustive, and you should identify adequate and cost-effective controls that are specific to your Mission environment. If you require assistance, send e-mail to the **ISSO@usaid.gov**. Each threat has a set of associated, pre-populated basic controls and mitigating actions.

Natural Threats	Preventative Controls	Mitigating Action
Earthquake	Off-site storage of backup media and system documentation Personnel safety and evacuation plans	Relocate to another Mission Relocate to USAID/W
Fire	Fire detection and suppression system Fireproof containers for backup media and system documentation Off-site storage of backup media and system documentation Personnel safety and evacuation plans	Relocate to another Mission Relocate to USAID/W
Flood	Water detection and notification system Off-site storage of backup media and system documentation Personnel safety and evacuation plans	Relocate to another Mission Relocate to USAID/W
Storm	Water and fire detection, notification and suppression systems Off-site storage of backup media and system documentation Personnel safety and evacuation plans	Relocate to another Mission Relocate to USAID/W
Manmade Threats	**Preventative Controls**	**Mitigating Action**
Arson	Fire detection and suppression system Fireproof containers for backup media and system documentation Off-site storage of backup media and system documentation	Setup up hardware and restore from backups Relocate to another Mission Relocate to USAID/W
Civil Unrest	Guard services Personnel safety and evacuation plans	Relocate to another Mission Relocate to USAID/W
Sabotage	Physical access controls Intrusion detection and notification systems Off-site storage of backup media and system documentation	Relocate to another Mission Relocate to USAID/W
Terrorism	Guard services Physical access controls Intrusion detection and notification systems Personnel safety and evacuation plans Off-site storage of backup media and system documentation	Relocate to another Mission Relocate to USAID/W

Theft	Physical access controls Intrusion detection and notification systems	Setup up hardware and restore from backups
Environmental (Non-Data) Threats	**Preventative Controls**	**Mitigating Action**
Air Conditioning Failure	HVAC out-of-range detection and notification system Redundant HVAC system	Service level agreements with facilities vendor
Electrical Power Failure	Automatic backup generator Redundant electrical circuits Uninterruptible power supplies Emergency shutdown switches	Service level agreements with utilities vendor
Equipment Failure	Redundant Equipment (cold spares) Redundant Equipment (hot spares)	Service level agreements with vendor
Telecommunications Failure	Alternate telecommunications pathway (ISP, VSAT) Backup communications circuit (land-line)	Service level agreements with communications vendor
Environmental (Data) Threats	**Preventative Controls**	**Mitigating Action**
Record or Data Loss	Technical security controls	
Disclosure of Information	Technical security controls	
Mission Specific Threats	**Preventative Controls**	**Mitigating Action**

This chart contains threats and their related controls and mitigating actions.

There are additional items from formal Business Continuity and Disaster Recovery Planning that should be included when you plan. These include notification lists (who do you need to notify when there are potential or actual interruptions of service?), activation criteria (when, under what conditions, are you going to activate your plan?), annual validation (does everything still work?), etc. If you have any questions, please send e-mail to **ISSO@usaid.gov**.