**BUSINESS IMPACT ANALYSIS**

1. ***Introduction***

As an essential part of Continuity Risk Management Activities, the Business Owners must conduct a business impact analysis (BIA) every two (2) years to document the business impact of a service disruption to the mission of CMS. The BIA is developed to:

* + Validate alignment with CMS Mission Essential Functions (MEFs) and Essential Supporting Activities (ESAs)
	+ Determine the criticality of mission/business processes through an all-hazards risk analysis
	+ Identify risk mitigation and recovery strategies based on criticality
	+ Identify resource requirements needed to resume mission/business processes and related interdependencies (facilities, personnel, equipment, software, data files, system components, and vital records)
	+ Identify recovery priorities for sequencing recovery and resources

The BIA should help inform the Contingency Planning process in identifying preventive controls for the functions and resources, and in developing the Contingency Plan.  It should serve as a starting point for the disaster recovery planning and define key parameters such as maximum tolerable downtime (MTD), recovery time objectives (RTO),  recovery point objectives (RPO) and resources/materials needed for business continuity.  It should also be used to support the development of other continuity plans associated with the function, including, but not limited to, Incident Response Plan (ORP), Business Continuity Plan (BCP), and Continuity of Operations Plan (COOP).

1. ***Purpose***

This paper describes the process that should be performed by Business Owners and relevant stakeholders when developing a business function BIA.

1. ***Scope***

This paper describes the steps leading to successful development of a business function BIA and addresses the roles and responsibilities of the stakeholders involved in.

1. ***Roles and Responsibilities***

The following definitions of the roles and responsibilities identify the key stakeholders and their actions in developing a business function BIA.  These definitions follow the pattern established by ISPG in the ELMO business function BIA development.

**Business Owner:**  has primary responsibility for the BIA, including development and ongoing maintenance.  This includes writing the BIA report and holding working sessions to collect information and to achieve consensus on the details, including impacts from potential threats and hazards.

**System Owner and other associated Subject Matter Experts (SMEs):**  will provide support to the development and ongoing maintenance.  The SMEs include groups such as OIT that provide a wider perspective, especially for impacts to CMS related or interdependent funcions.  SME’s also help formulate more efficient and effective mitigation strategies.

**Continuity Program:**

* + Will provide support to the development and ongoing maintenance in the form of templates and guidance on how to do a business function BIA.  This support can include direct involvement in the BIA working sessions to guide the BIA team on the details of the BIA content.  It can also include providing comments and reviews that help maintain the level of detail and content across CMS.
	+ Will provide monitoring and verification that BIAs are completed as part of the CMS eXpedited Life Cycle (XLC) process for new developments, are regularly maintained as part of the CMS change management process, and are updated at least every two years.

**CMS Leadership:**  will review the BIA findings and verify the risk based analysis and mitigation strategies reflect the needs of CMS.

1. ***Critical Timeframes***

The BIA process should be integrated into the existing CMS processes including the eXpedited Life Cycle (XLC) and the change management process.  This ensures the BIA is initially completed and verified before the business function is deployed in production.  It also ensures changes to the business function occurring over time are evaluated for impacts to the BIA and updates due to these impacts are routinely completed.

The BIA development should begin during the  Initiation, Concept, and Planning phase of the XLC.  These actions include the initial discussions around the new function’s relationship to the CMS MEFs, ESAs, and the CMS risk analysis.  Risk mitigation strategies are proposed and initial values for MTD, RTO,  RPO, and resources/materials needed for business continuity are defined.

The BIA development should continue into the Requirements Analysis and Design phase of the XLC.  As the business function design matures and trade-offs are incorporated, the BIA needs to be reviewed for impacts these trade-offs and changes may require.  These continuing reviews ensure the BIA represents the final business function design.  It is during this phase that the Contingency Plans (CPs) for the supporting infratstructure are developed based on the final BIA.

The BIA and the CPs should be verified during the Development and Test phase of the XLC.  Parameters such as the MTD, RTO, and RPO should be verified or changed to reflect the final business function capabilities.

The BIA should be reviewed every two (2) years and/or updated when changes are made to the business function as part of the Operations & Maintenance and Disposition phase of the XLC.  This is when the CMS change management cycle becomes the key to ensuring the BIA is always updated to reflect the current business function design.  The change management cycle should have hooks that cause an analysis of impacts to the BIA to be performed for all proposed function changes.  All the steps should be completed for the review every two years or for updates due to changes.

1. ***BIA Process Steps***

The initial step in developing the BIA is to determine the MEFs and ESAs for CMS.  Once leadership establishes the MEFs and ESAs, the business function in the BIA can be aligned with the relevant MEFs and ESAs or can be identified as a function that is not aligned.  These determiniations can then be used as the basis for the risk analysis and mitigation planning.  This ensures an acceptable level of risk is maintained across CMS while at the same time, CMS resources are assigned as efficiently and effectively as possible.

The following steps should be performed to fill out the BIA template.  The various stakeholders and SMEs associated with the business function should be brought into the BIA process as required, including the Continuity Program for templates and guidance, plus OIT and the system maintainer/DR vendor for consultation and concurrence for technology.

**Step 1:**  Collect the details describing the business function.  This collection represents the Business Process Analysis (BPA) portion of the BIA.  These details include function alignments with MEFs and ESAs, outputs and inputs, dependencies, identification of leadership and required staff, communications and information systems, alternate location requirements, and identification of resources and funding to perform the business function.

**Step 2:**  Perform an all-hazards risk analysis that considers risks posed by all conditions, environmental or manmade, that have the potential to cause injury, illness, or death; damage to or loss of equipment, infrastructure services, or property; or causing functional degradation.  Applicable threats and hazards must be analyzed against the business function elements, including interdependencies, to determine the extent of impacts of business function failure.

The analysis may be performed by following the steps shown in the BIA template to consider a wide range of threats and hazards.  Or the analysis may be performed using a CMS level risk study, if available.

The analysis may be performed as a series of working sessions with representatives of the business along with a variety of SMEs from around CMS so that each threat and hazard can be thoroughly evaluated for its impacts on the people, processes, and technology involved with the business function.

The outcome is a list of threats and hazards that need to be mitigated in order to meet the performance requirements of the business function while maintaining an acceptable level of CMS risk.

**Step 3:**  Develop mitigation plans for the identified threats and hazards that can be implemented within the constraints of CMS, including people, process, technology, and budget.  Also develop a description of the remaining risk assuming the mitigation is properly implemented.  For example, if the threat is a failure of an IT system, the mitigation plan may be for OIT to recover the system within 12 hours.  The remaining risk that needs to be communicated to Leadership is the business function can be lost for up to 12 hours.  Is this an acceptable risk to CMS?

**Step 4:**  Review the draft BIA with CMS Leadership and gain concurrence on the mitigation plans and on the remaining level of risk.

**Step 5:**  Release the BIA across CMS for use by the other stakeholders and processes across CMS.  For instance, the key parameters and mitigation strategies represent performance requirements for organizations such as OIT and service levels for support provided by the function to other business functions.