**BUSINESS IMPACT ANALYSIS (BIA) FOR BUSINESS FUNCTION**

|  |  |  |
| --- | --- | --- |
|   |  **CMS Disaster Recovery** |   |
|   |  **Y/N** |  **Comments/Details required for DR** |   |
|  **DR Required?** |   |   |
|  **Mitigation Required?** |   |   |
|  **BCP/COOP Required?** |   |  **Comments/Details/ Equipment Dependencies** |
|   |
|  **Business Function Cross-Reference** |   |
|  **BIA Meeting Date** |   |
|  **BIA Facilitated By** |   |

**Blue text is instructional text.**

1. ***Identify System Points of Contact***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  **Points of Contact** |  **Name and Title** |  **Critical to Completing the Process** **(Yes, No / Subject Matter Expert)** |  **Office #** |  **Cell #** |
|  Leader |   |   |   |   |
|  Backup Leader |   |   |   |   |
|  Team Members (Repeat row as needed) |   |   |   |   |
|  Vendor Information |   |   |   |   |
|  Alternate Work Location |   |   |   |   |
|  **Conference Bridge Information** |  **Numbers** |   |
|  Domestic Dial-In Number: |   |
|  International Dial-In Number: |   |
|  Conference Code: |   | **Leader Pin #:** |   |
|  **GAL Distribution Lists** |
|   |   |

Identify the individuals, positions, or offices within and outside of your organization that depend on or support the system, also specify the relationship to system.

**Complete the following table before or after the BIA working sessions.  Copy the table for each critical process.**

***Overview and Critical Business Processes***

This section is provided to focus on your business function only. Section 4 is to be used for identifying those systems/applications that your business function has a dependency on or that depends on your business function.

Document all the functions performed in the following table to establish a complete list of functions or services provided by the Business Owner.  Work through the list and identify the essential functions, criticality of essential functions, and the purpose and process of the application. Include the Mission Essential Functions (MEFs), Essential Supporting Activities (ESAs), criticality of essential functions, supporting infrastructure, and other resources**.**

**The CMS Mission Essential Functions (MEFs) are:**

1. Cash Flow to external stakeholders to prevent lapses in health care coverage.
2. Enrollment of individuals in Medicare, Medicaid, and Children’s Health Insurance Program (CHIP), and in private health care plans through the Health Insurance Marketplace.
3. Communication of health, policy, and emergency information to internal and external stakeholders.
4. End Stage Renal Disease (ESRD) patient and facility tracking.
5. Quality Care for CMS program beneficiaries.

**The Essential Supporting Activities (ESAs) at CMS are:**

* Managing time keeping, payroll, and travel.
* Managing necessary facilities, security, badging, and building access.
* Implementing and communicating human resource policies to the workforce.
* Coordinating and communicating with stakeholders and other U.S. Government agencies.
* Managing and maintaining necessary basic communications (telephonic, FAX, email).
* Supporting IT infrastructure for the Agency’s MEFs and ESAs.
* Receiving and distributing Agency mail and deliveries.
* Performing legal reviews, contract oversight and data analysis.
* Managing essential records and correspondence.
* Conducting emergency and continuity coordination activities.
* Other supporting activities identified through the Business Impact Analysis (BIA) process.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|   | Function Performed by the Application | Which MEFs or ESAs does it support | Identify any Critical deadlines / time periods in the system Cycle | Critical Dependencies or resources needed  | Identify any functions or systems that are dependent on this function |
| **1.** |   |   |   |   |   |
| **2.** |   |   |   |   |   |
| **3.** |   |   |   |   |   |
| **4.** |   |   |   |   |   |
| **5.** |   |   |   |   |   |
| **6.** |   |   |   |   |   |
| **7.** |   |   |   |   |   |
| **8.** |   |   |   |   |   |
| **9.** |   |   |   |   |   |
| **10.** |   |   |   |   |   |
| **11.** |   |   |   |   |   |
| **12.** |   |   |   |   |   |
| **13.** |   |   |   |   |   |
| **14.** |   |   |   |   |   |
| **15.** |   |   |   |   |   |
| **16.** |   |   |   |   |   |
| **17.** |   |   |   |   |   |
| **19.** |   |   |   |   |   |
| **20.** |   |   |   |   |   |

|  |  |
| --- | --- |
| Investigation, Intelligence-Related, And Security Information (14 CFR PART 191.5(D)) | Information related to investigations for law enforcement purposes; intelligence-related information that cannot be classified, but is subject to confidentiality and extra security controls. Includes security plans, contingency plans, emergency operations plans, incident reports, reports of investigations, risk or vulnerability assessments certification reports; does not include general plans, policies, or requirements. |
| Mission-Critical Information | Information and associated infrastructure directly involved in making payments for Medicare Fee-for-Service (FFS), Medicaid and State Children’s Health Insurance Program (SCHIP). |
| Information About Persons | Information related to personnel, medical, and similar data. Includes all information covered by the Privacy Act of 1974 (e.g., salary data, social security information, passwords, user identifiers (IDs), Equal Employment Opportunity (EEO), personnel profile (including home address and phone number), medical history, employment history (general and security clearance information), and arrest/criminal investigation history as well as personally identifiable information (PII), individually identifiable information (IIF), or personal health information (PHI) covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). |
| Financial, Budgetary, Commercial, Proprietary And Trade Secret Information | Information related to financial information and applications, commercial information received in confidence, or trade secrets (i.e., proprietary, contract bidding information, sensitive information about patents, and information protected by the Cooperative Research and Development Agreement). Also included is information about payments, payroll, automated decision making, procurement, market-sensitive, inventory, other financially-related systems, and site operating and security expenditures. |
| Internal Administration | Information related to the internal administration of an agency. Includes personnel rules, bargaining positions, advance information concerning procurement actions, management reporting, etc. |
| Other Federal Agency Information | Information, the protection of which is required by statute, or which has come from another Federal agency and requires release approval by the originating agency. |
| New Technology Or Controlled Scientific Information | Information related to new technology; scientific information that is prohibited from disclosure or that may require an export license from the Department of State and/or the Department of Commerce. |
| Operational Information | Information that requires protection during operations; usually time-critical information. |
| System Configuration Management Information | Any information pertaining to the internal operations of a network or computer system, including but not limited to network and device addresses; system and protocol addressing schemes implemented at an agency; network management information protocols, community strings, network information packets, etc.; device and system passwords; device and system configuration information. |
| Other Sensitive Information | Any information for which there is a management concern about its adequate protection, but which does not logically fall into any of the above categories. Use of this category should be rare. |
| Public Information | Any information that is declared for public consumption by official authorities.  This includes information contained in press releases approved by the Office of Public Affairs or other official sources.  It also includes Information placed on public access world-wide-web (WWW) servers. |

1. ***Critical Business Process Performance***

Explain the mission critical business processes that support your organization.  This should include all your business processes.  Once those are documented, define a process owner and a general recovery objective (more detailed peak times should be defined in the next section). Analyze the impact(s) the function’s disruption will have to the MEFs and the information type(s) processed by the function. The following 11 information types should be used when considering each function:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Critical Business Process(es)** |  **Information Type(s)** | **Process Owner****(Department)** | **Recovery Time Objective (RTO)** | **Recovery Point Objective (RPO)** |
|   |   |   |   |   |

1. ***Business Process Critical Time Information***

Document the critical peak times of any day, week, month, or year for the business function.  For instance, these times include when batch jobs are normally processed, when periodic workloads such as end of month financial applications are needed, or when an open enrollment period occurs.

|  |
| --- |
| **Critical time of day / month / year / project** |
|    |

1. ***Application Dependency***

Document any applications, systems, or other resources required for continuing critical business processes during an outage. Is the function fully reliant on any/all of these dependencies for continued operation? Describe the relationship between the function and each dependency.

Describe the business process and data that your function relies on from each dependency.

Identify the necessary recovery time needed for each dependency that affects your function and business process(es). How long will it take to have a major impact to the operation of your function’s business process(es) i.e. minutes, hours, days, weeks, and/or months (System Downtime and Age of Data)?

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Software/ Application/System** | **Description** | **CMS Controlled Only? (Y/N)** | **Is There a Documented Backup Plan? (Y/N)** | **System Downtime** | **Age of Data** |
|   |   |   |   |   |   |
|   |   |   |   |   |   |

1. ***Other Requirements / Dependencies Not Identified Above***

Document any additional requirements, such as indirect support, for continuing critical business processes during an outage.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Software/ Application/System** | **Description** | **CMS Controlled Only? (Y/N)** | **Is There a Documented Backup Plan? (Y/N)** | **System Downtime** | **Age of Data** |
|   |   |   |   |   |   |
|   |   |   |   |   |   |

1. ***Key Support Personnel***

Include contact information of CMS staff, other agencies and vendors who provide both direct and indirect support for the critical processes, applications, and systems.  Is the vendor a sole source vendor for your function and do they have a Business Continuity Plan (BCP)?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Service Description** | **Sole Source Vendor? (Y/N)** | **Does The Vendor Have A BCP? (Y/N)** | **Does a Service Level Agreement exist? (Y/N)** |
|   |   |   |   |   |
|   |   |   |   |   |

1. ***Ongoing Business Changes***

Document any ongoing or planned changes that could impact the business functions or supporting resources. Describe the change and the estimated impact to the Critical Business Process(es) identified in Section 2, including the schedule for the planned changes.

|  |  |
| --- | --- |
| **Description of the Change** | **Estimated Impact** |
|   |   |

1. ***Business Function Information***

Provide a general description of the business function and the associated system architecture.  From start to finish, describe how the function is performed.  Include information about who it serves, what it produces, what it needs, etc.

For the associated information system Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems.  Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures.

Note: Information for this section should be available from the system’s System Security Plan (SSP) and can be copied form the SSP or reference the applicable section in the SSP and attach the latest version of the SSP to this BIA. Please consult your system maintainer for assistance, if necessary.

|  |
| --- |
| **Description** |
|   |

1. ***Identify Information System Requirements***

Document any identified application specific information  including hardware, software, and other resources such as data files needed to support the <insert system name> mission/business processes identified in Section 2, unless otherwise stated.  Information for this section should be available from the system’s SSP. Please contact your system maintainer for assistance, if necessary.

|  |  |  |
| --- | --- | --- |
| **Hardware Name** | **Hardware Type** | **Description** |
|   |   |   |

|  |  |  |
| --- | --- | --- |
| **Software Name** | **Software Type (Platform/OS/Version as applicable)** | **Description** |
|   |   |   |

|  |  |  |
| --- | --- | --- |
| **Data File Name** | **File Type** | **Description** |
|   |   |   |

1. ***Backup Strategy***

Document scheduled data backups required for continuing critical business processes during an outage. Identify the backup location such as Cloud, Data Center, or Manual.

|  |  |
| --- | --- |
| **Back-up Types** | **Backup Schedule/Frequency(s)** |
|   |   |
|   |   |
|  |  |

1. ***Identify Order of Recovery for System Resources***

Document the order of recovery for system resources.  A system resource can be software, data files, servers, or other hardware and should be identified individually or as a logical group.

|  |  |  |
| --- | --- | --- |
| **Priority** | **System Resource/Component** | **Maximum Tolerable Downtime** |
|   |   |   |
|   |   |   |
|   |   |   |

1. ***Additional Information***

*Please provide any additional information you would like to share concerning backup and recovery needs.*

|  |
| --- |
| ***Description*** |
|   |

1. ***Business/Mission Process Risk Assessment***

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 in this 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 CMS level risk study can be reviewed in place of the following table with the results of the review recorded in Section 15.

Use the following definitions when analyzing each hazard and threat.  Use these terms to fill in the appropriate columns in the table below.

|  |
| --- |
| ***Likelyhood of Occurrence*** |
| **Low** | ***Unlikely:*** An event/condition that can be envisioned but hasn't occurred (~20% chance over the foreseeable future) |
| **Moderate** | ***Possible:*** An event/condition that has occurred in the past (50:50 over the foreseeable future) |
| **High** | ***Likely:*** An event/condition that has occurred in the past at a frequency warranting its anticipation in in the near future (>75% chance) |
|   |   |
| ***Impact on Business function*** |
| **Low** | ***Little Impact:*** Any outage with little impact, damage, or disruption to the organization. |
| **Moderate** | ***Important/Moderate Impact:****Any system that, if disrupted, would cause a moderate problem to the organization and possibly other networks or systems.* |
| **High** | ***Mission-critical Impact:*** The damage or disruption to the system would cause the most impact on the organization, mission, and other networks and systems. |

|  |  |
| --- | --- |
| **Risk Decision** | **Description** |
| Accept | Do nothing |
| Mitigate | Implement physical or procedural controls to reduce the impact or likelihood of a disruption |
| Plan / Develop BCP/COOP | Pre-plan response to minimize effects of a disruption (i.e. develop a BCP/COOP) |
|    |   |

***Use the following overall risk – decision matrix to consider the planned mitigations or actions to take in support of the function.***

|  |
| --- |
| **Overall Risk - Decision Matrix** |
| **Likelyhood** | **High** | **Mitigate & Develop BCP** | **Mitigate & Develop BCP** | **Mitigate & Develop BCP** |
| **Moderate** | **Mitigate & Develop BCP** | **Mitigate & Develop BCP** | **Mitigate & Develop BCP** |
| **Low** | **Accept** | **Mitigate & Develop BCP** | **Mitigate & Develop BCP** |
|   |   | **Low** | **Moderate** | **High** |
|   |   | **Business Impact** |

***The following table lists potential threats and hazards to consider.  Add additional threats and hazards as needed.***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Potential Threats and Hazards** | **Potential Impact to CMS** | **Describe Business Function Impact** | **Information Type(s) Impacted** | **Likelyhood** | **Impact** | **Risk Decision** | **Proposed Mitigations / Actions** |
| **Infrastructure Attack/Failure/Damage** |   |   |   |   |   |   |   |
| IT System Crash | Function stops operating |   |   |   |   |   |   |
| Power Outage (Regional Blackout) | Power is lost |   |   |   |   |   |   |
| Communications System Disruption (wide area network, local area network, voice network, cell network) | Communications is lost |   |   |   |   |   |   |
| Heating/Air Conditioning Failure | Temperatures become uncontrollable |   |   |   |   |   |   |
|  |  |  |  |  |  |  |  |
| Ventilation System Failure | Intake of fresh air and exhaust of stale air is lost |   |   |   |   |   |   |
| Transportation System Disruption | All or some roads become impassable around HQ |   |   |   |   |   |   |
| Major Fire | All or some of HQ and surrounding area is destroyed |   |   |   |   |   |   |
| Water Supply Contamination | No water is available for consumption |   |   |   |   |   |   |
| Sewage System Failure | Plumbing stops functioning |   |   |   |   |   |   |
| **Cyber Attack** |   |   |   |   |   |   |   |
| Insider Threat, sabat | All or some HQ systems are impacted |   |   |   |   |   |   |
| Loss of Data or Network Service Disruption | All or some HQ systems are impacted |   |   |   |   |   |   |
| Control Systems Failure | All or some HQ systems are impacted |   |   |   |   |   |   |
| **Natural Disaster** |   |   |   |   |   |   |   |
| High Wind (Hurricane, Tornado) | All or some of HQ and surrounding area is destroyed |   |   |   |   |   |   |
| Winter Storm | Transportation in HQ area is shutdown |   |   |   |   |   |   |
| Major Earthquake | All or some of HQ and surrounding area is destroyed |   |   |   |   |   |   |
| Floods | All or some of HQ and surrounding area is destroyed |   |   |   |   |   |   |
| Drought | None |   |   |   |   |   |   |
| Volcanic Eruption | None |   |   |   |   |   |   |
| Tsunami | None |   |   |   |   |   |   |
| Wildfire | None |   |   |   |   |   |   |
| Solar Weather | None |   |   |   |   |   |   |
| **External Threats and Hazards** |   |   |   |   |   |   |   |
| **Explosions**:  Nuclear Attack, Radiological Dispersal Device,Improvised Explosive Device, Incendiary Device | All or some of HQ is destroyed |   |   |   |   |   |   |
| **Active Shooter:**  Disgruntled Employee, terrorist attack | HQ in lock-down |   |   |   |   |   |   |
| **Chemical/Biological:**Biological Attack/Outbreak, Aerosol Anthrax; Plague, Food Contamination, Animal Disease, Pandemic Influenza; Chemical Attack/Accident, Toxic Industrial Chemicals, Chlorine Tank Explosion | All or some of HQ is evacuated or uninhabitable |   |   |   |   |   |   |
| **Labor/Insurrection:**  Civil Unrest;  Labor Dispute, Workforce Strike;  | Personnel are not available at HQ |   |   |   |   |   |   |
| **Economic:**  Economic Catastrophe (market crash, loss of confidence) | Ability of CMS to provide services is questioned |   |   |   |   |   |   |
| Supply Chain Failure | Vendors fail to deliver required supplies |   |   |   |   |   |   |

***Timeframe for Unacceptable Loss of Functions***

Analyze and determine acceptable versus unacceptable downtimes for business functions and supporting resources.  Based on the risk analysis in the previous section, list each function or resource requiring mitigation or other actions in the following table.

Determine the following parameters assuming the planned mitigations or actions are in place and operating.  These parameters represent requirements for organizations supporting the business function, such as OIT.  The parameters also represent service levels that can inform downstream functions of what to expect.

* + Documented Backup Plan:  describe the backup plan implemented to support the function.  This should include frequency, storage period, and locations for all copies.
	+ Recovery Point Objective (RPO):  is the maximum acceptable level of data loss following an uplanned event.  This should align with the Backup Plan.
	+ Maximum Tolerable Downtime (MTD): the maximum amount of time acceptable for a disruption to or degradation of business function performance. Consideration must be given to the impact of downtime on supporting infrastructure and activities, including the estimated duration of a resource loss before it affects the MEF it supports.
	+ Recovery Time Objective (RTO): assign an RTO considering the MTDs for the function(s) it supports. An RTO is a value describing the maximum amount of time that a resource requirement or critical asset can be unavailable before it has a failure impact on essential functions.
	+ Remaining Risk:  describe the remaining risk and performance limitations after the mitigations and actions have been implemented.  For instance if a system can be recovered within a 12 hour window, then the remaining risk is a loss of business function for less than 12 hours.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Business Function or Resource** | **Documented Backup Plan** | **RPO** | **MTD** | **RTO** | **Remaining Risk** |
|   |   |   |   |   |   |

1. ***Summary of Potential Impacts***

Summarize the potential impacts to the business functions and supporting resources.  This will be used to inform decision making on resource allocation and to manage risks.

|  |
| --- |
| ***Summary*** |
|   |