E. **Emergency Response and Disaster Recovery Plan**
Describe the Vendor's proposed emergency response and disaster recovery plan, including a summary of how the plan addresses the following areas:

Humana's corporate Disaster Recovery (DR), Cybersecurity, Crisis Management, and Business Continuity (BC) plans guide our responses to threats to our data integrity, data security, and business operations. Tested annually, these plans have proven effective in actual emergencies; for example, execution of these plans guided our emergency response to Hurricane Irma in Florida that resulted in swift resumption of services to providers and Enrollees.

Humana deploys state-of-the-art hardware and software to ensure ongoing system performance at the highest level. We use Hewlett Packard's OpenView and SolarWinds Orion software for large-scale system and network management to measure end-to-end performance, diagnose any bottlenecks, preempt availability-threatening failures, and add capacity as utilization approaches thresholds. We supply multiple paths from different carriers to ensure safe and secure online connections with our internal operations. At a corporate level, our wide area network (WAN), campus local area network (LAN), telecommunications infrastructure, and secure dual data centers have the redundancy, scalability, and security to meet state requirements and respond to emergencies.

Humana meets and often exceeds Centers for Medicare and Medicaid Services (CMS) Essential Functions Guidelines in limiting service interruption to 24 hours for Tier I applications in a disaster event. Through our DR plan, we maintain processes for archiving and restoring data in the event of a system or subsystem failure. We retain three copies of our critical systems, so we can mitigate issues if one of the copies is damaged or destroyed. Application teams perform backups of critical servers and critical data at the file level nightly in the event some subset of the replicated data becomes corrupt. The DR team has six full-time consultants and one team manager, representing a combined total of more than 100 years of experience in information technology (IT), including extensive background with Humana systems.

1. Essential operational functions and responsible staff members

As described in Humana's Disaster Recovery Plan, "The company exists to make positive contributions to our customers' good health and well-being by providing affordable health solutions tailored to meet specific needs." Our essential operational functions are those that enable us to sustain this mission in the face of a disaster. While somewhat

dependent on the nature of the disaster, **essential operational functions are those activities that support the continuation of health services to those Enrollees under care and the initiation of health services to those who present with a need**. Humana's communication mechanisms and information systems are vital to supporting healthcare providers and their patients in such situations.

[redacted]

Humana's robust infrastructure contains applications and services that are critical to technical and data center operations. We duplicate these applications and services at the secondary data center (SDC). Data replication for applications defined as Tier 1 (catastrophic/must have) occurs between both our data centers over private encrypted data links so the data never leaves corporate secure facilities. We perform backups of critical servers and critical data at the file level as requested or as scheduled by the application teams. For mission critical systems, Humana often retains three copies of production data. Two are at the main data center, and the third is at the alternate site. This structure mitigates loss if one copy of data is damaged or destroyed.

DR testing occurs throughout the year. We conduct most of these tests at the alternate data center using an "in-house" DR strategy, although contracted hot-site vendor facilities conduct some testing for remote facilities. Humana documents and maintains all testing results for future review.

2. Plans to ensure critical functions and continuity of services to Providers and Enrollees will be met

Humana has designed its DR and BC plans to guide technical response teams and business owners in the continuation of critical functions for providers and Enrollees during disasters and the immediate recovery period. These critical functions include the personnel, data, and physical structures necessary to maintain services for providers and Enrollees. **These services fall into broad categories: lines of communication between and among Humana associates, providers, and Enrollees; authorization of critical services; and payment for certain critical services**.

To maintain communications in the event of a disaster, associates working from home or in alternate locations will restore the Member Services and Provider Services Call Centers. To function properly, call centers rely on data regarding Enrollees, providers, clinical history, service authorizations, and payments. Humana supplies secured access to business-critical applications and virtual desktops for our associates, business partners, and software developers. We employ an active-active model for critical systems in our two data centers, which enables us to host capacity at a single data center in case of a disaster recovery situation. Virtual applications are securely hosted on Citrix infrastructure, allowing authenticated users to access back-end data while keeping all data and interactions within our corporate walls. The data center also hosts virtual desktops, which allows users to access Humana-imaged desktops from any device anywhere and at any time, while keeping all data secure.

We house all production servers in Humana's primary hardened data center 20 miles south of our corporate headquarters in Louisville, Kentucky. Our secondary data center, located in Simpsonville, Kentucky, offers redundancy and can be activated remotely. As a result of our system security protections, Humana has never experienced a loss of data due to a system or program failure or destruction. We maintain backups of critical applications and systems, which we update nightly. Our data centers are accessible remotely by authorized associates via Humana's secured virtual private network (VPN), which allows us to maintain operational functionality regardless of time or place. Both data centers are Tier III-certified; they require no shutdowns for equipment replacement and maintenance, they have exterior walls built to withstand 150 mile-per-hour winds, and they are windowless in the area storing data.

Maintaining network capabilities is critical during disasters. The Network Services team is responsible for procuring computer equipment for the primary data center site and for the alternate recovery site, building new equipment that meets required specifications for replacing damaged equipment, and assisting in new

equipment installations to meet the required Recovery Time Objectives (RTO) following a disaster. The LAN Operating Systems team, which also plays a critical role in all recovery processes, is responsible for providing server configuration templates to the Configuration Center and operational procedures for LAN operating systems to all company sites.

In disaster situations, providers may not have access to their facilities or be able to provide authorizations that are normally required for prescriptions, specialty consultations, or surgeries. Humana has the systems in place to waive such authorizations. For example, during Hurricane Irma, due to the Crisis Management team's daily disaster monitoring duties, we were able to automatically waive edits such as "refill too soon" for prescriptions and out-of-network provider authorizations for Enrollees in specific areas.

Similarly, payment authorizations may be required for certain services even though all preconditions may not be met due to the disaster situation. We have designed payment controls to be waived in such situations, with appropriate reconciliation after the situation has stabilized.

3. Staff training

Members of the DR team responsible for DR plans and testing are certified by DRII.org, which is an international body for educating and credentialing on disaster recovery and business continuity. Our associates maintain their certification and membership in that organization via continuing education. Continuing Education Activity Points (CEAPs) are earned by associates through a variety of activities, including attending or speaking at professional conferences, developing company-supported educational workshops, publishing an article in a professional journal, and editing an internal newsletter. At any given time, at least one half of the DR team maintains certification with DRII.org. Team members also hold certifications from EMC for VMWare, SRM/SRDF, PMP, ITIL, Cisco, MCSE, and more.

The DR team offers four Humana training sessions to associates regarding DR, including:

- **DR fundamentals**: Overview of recovery-based activities; how we participate in IT disaster recovery discussions with our partners, stakeholders, and associates.
- **DR planning**: Recovery Plan development, ownership, and maintenance; Recovery Plan best practices, compliance reporting, escalation, and how to engage the IT Disaster Recovery team for support.
- **DR testing and exercises**: Disaster Recovery compliance requirements for plan and system testing and reporting; expectations during an actual disaster.
- **DR plan repository**: Use of the new, in-house tool, including creating and maintaining a plan in the repository, automated notifications, approvals, and reporting.

The Enterprise Resiliency Standard provides the framework and guidelines for business continuity plan exercises across the enterprise. Business Continuity Plan Owners and Recovery team members within each market participate in annual exercises of their Business Continuity Plan. These exercises include different loss type scenarios such as facility, people, technology, and vendor. The Crisis Management team and Enterprise Critical Incident Response Team (ECIRT) conduct other exercises such as active shooter, hurricane response, cyber response, and other natural or man-made disaster response. These exercises ensure associates are trained on their roles and responsibilities during a disruptive event.

The Enterprise Business Continuity team has developed technology-based training videos to ensure associates are trained on the importance of Business Continuity planning (particularly in the context of the scenarios described above) as well as the overall related lifecycle. Specific topics covered by these videos include:

- Introduction to the Enterprise Resiliency Office (four modules):
  - Business Impact Analysis
  - Strategy and Plan development
  - Crisis Management and communication
  - Plan Exercises

- Crisis Management Overview
- Humana Business Continuity Plan table top exercise – Severe Weather
- Humana – Pandemic BC exercise
- Humana – Network outage BC exercise
- Humana – Vendor outage BC exercise

The Enterprise Risk Management team provides oversight to ensure required staff training is completed on an annual basis.

Humana believes in leveraging learnings and experience at all levels to support continuous business process improvement. After each event and training exercise, leaders at headquarters and in market locations conduct "lessons learned" reviews of the response. Best practice learnings from these reviews are incorporated into subsequent training programs and business continuity plans.

4. Contingency plans for covering essential operational functions in the event key staff are incapacitated or the primary workplace is unavailable

If there are no trained resources at other Humana locations or processes are paper-based, we identify a local, physical recovery site to resume business operations. Business areas may use this strategy in conjunction with "redirect" if redirection of work does not provide sufficient capacity to meet recovery timeline objectives. A business area may allow non-Work-at-Home (WAH) associates to work from home, assuming the associate has the required technology in place, their related business processes are electronic workflow-based, and their related business processes do not require incoming and/or outgoing correspondence. Business areas use this approach as their last option, as the event could have occurred during business hours and onsite associates and/or personal computers (PC) are not available after event, and/or work PCs are not available via remote desktop.

If allowing a non-WAH associate to work from home is not possible because the associate's home environment is affected by the disaster, business processes are redirected to associates and/or business processing locations not affected by the event. If business processes cannot be redirected to associates or performed by other locations, business leaders would work with Humana's ECIRT and Crisis Management team to relocate associates and needed equipment. Relocation of associates would be prioritized based on the Maximum Allowable Downtime of the business process and critical processing times (i.e., open enrollment, bids, etc.). Based on the situation, affected associates may be relocated to:

- A nearby Humana facility
- A nearby temporary office space
- A Humana facility or temporary office space outside of the affected city, county, state, or region

Associate safety is of paramount importance in our disaster response approach. In the Hurricane Irma recovery phase, Humana's first efforts were directed at identifying associates most affected by the storm. We deployed our employee assistance program, Helping Hands, to put those most affected in hotels to ensure they had safe places to stay. Those able to work did so from hotel rooms.

The table below displays a listing of business processes and the recovery approaches the business area may deploy over time to support an exercise or actual event. We have aligned these recovery approaches to the most recent Business Impact Analysis.

Table I.C.E-1: Contingency Planning for Appropriate Recovery Approach

Business Process	Workflow Type	Recovery Approach
Administration	Electronic	WAH (office-based associates)
Business Analytics	Electronic	WAH (office-based associates)
Care Management and Chronic Conditions	Electronic	Redirect-Permanent WAH
Clinical Innovations – Clinical	Electronic	Redirect-Permanent WAH
Enrollee and Community Education	Electronic	WAH (office-based associates)
Prior Authorization – Clinical Intake	Electronic	WAH (office-based associates)
Prior Authorization – Clinical Intake	Electronic	Redirect-alternate site
Prior Authorization – Clinical Review	Electronic	Redirect-alternate site
Quality – Clinical	Electronic	WAH (office-based associates)
Service Operations – Inbound Call Operation	Electronic	Redirect-alternate site
Service Operations – Inbound Call Operation	Electronic	Recover
Utilization Management – Clinical	Electronic	Redirect-Permanent WAH

The BC plan documents locations that currently perform the business function. We determine any redirect of work to other facilities at the time of event and based on the situation.

The Crisis Management team and ECIRT, which consist of executive-level management representatives from the various business lines, are accountable for:

- Providing guidance to support business decisions made during a crisis or extended downtime
- Allocating additional resources to support the recovery effort where needed
- Providing a liaison between and among external business partners, Enrollees, and the DR team to ensure we meet critical business needs during the recovery process
- Supporting corporate communications with information regarding the situation to publicly disseminate and report to various vendors, contractors, and providers
- Setting thresholds and making the determination to raise the incident response from crisis to disaster and if so, transferring management and recovery facilitation to the DR team

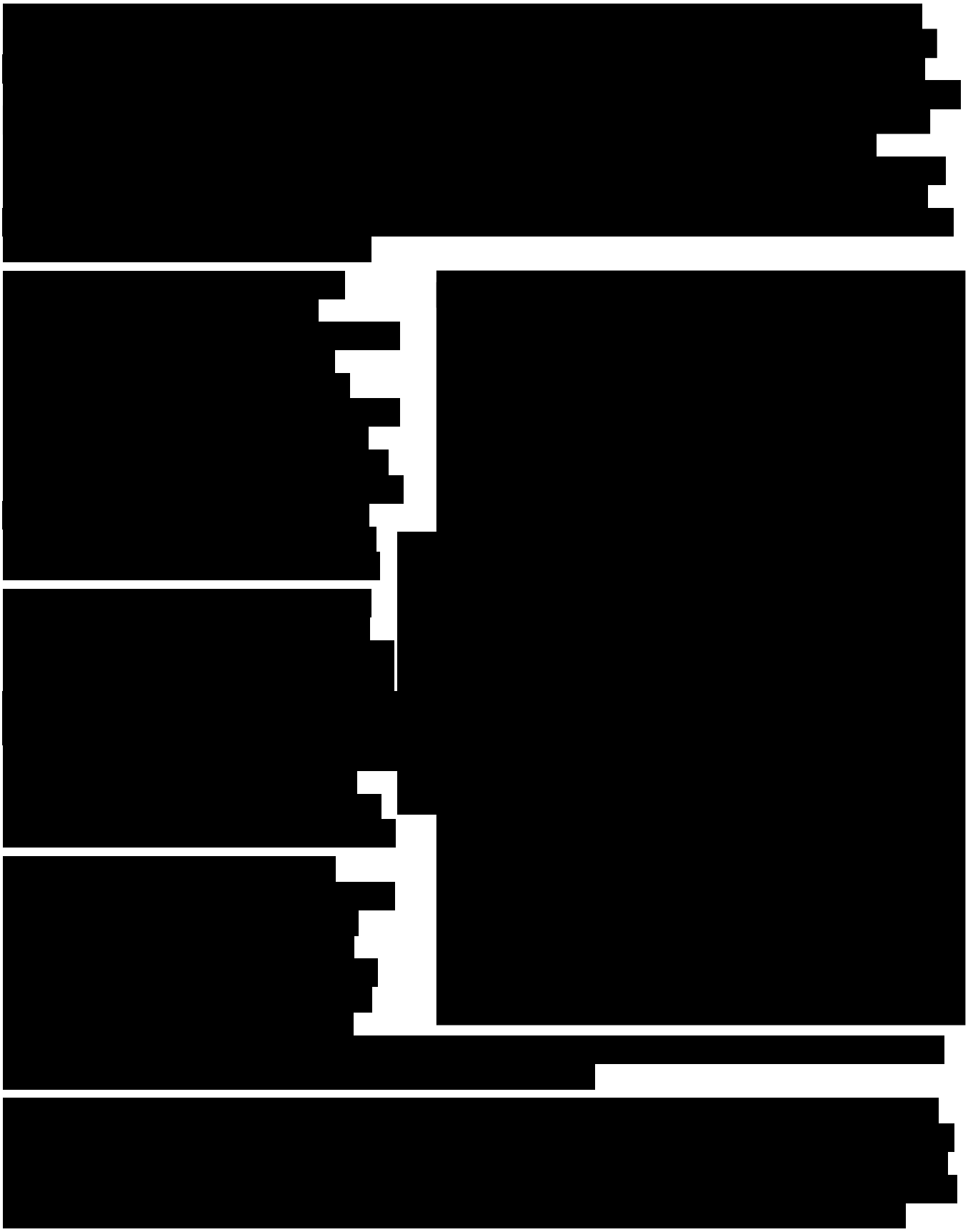
The Crisis Management team and ECIRT partner with business teams to determine and prioritize resources to support recovery efforts. Business areas are responsible for defining their specific business processes, defined as a collection of related procedures that address one or more business requirements. A business process has a well-defined beginning, end, and output. We also define a recovery approach or multiple recovery approaches for each business process. Business areas can redirect workflow queues and/or calls to an unaffected site (Humana or subcontractor) that has technology and trained associates to support work at a reduced capacity. Business areas can also rely on unaffected permanent WAH associates to support work.

5. Approach to maintaining data security during an event

Data security during an event falls into Tier 0, critical infrastructure, where there is zero downtime and zero data loss allowed. Our approach to data security is planned and organized to ensure that we are able to meet this critical infrastructure standard during an event.

Humana [redacted]

DATA SECURITY TECHNOLOGY



[redacted]

DATA SECURITY STANDARDS

We follow all state and federal laws and regulations. In the event of a conflict, the company follows the most stringent requirement. These regulations require that IT systems containing, using, processing, or storing PHI, financial, and Privacy Act data and doing business with the federal government have a documented DR plan defining how the organization continues its mission if service, use, or access to its computer resources is disrupted for 24 hours. These regulations include:

- ISO/IEC 27002:2013, Information Security Management – Code of Practice
- ISO/IEC 27001:2013, Information Security Management System
- ISO/IEC 22301:2012, Societal Security – Business Continuity Management Systems – Requirements

- ISO/IEC 24762:2008, Guidelines for Information and Communications Technology Disaster Recovery Services
- Sarbanes-Oxley Act of 2002, SOX
- HIPAA, 45 CFR Parts 160, 162, and 164, Health Insurance Reform: Security Standards
- CoBiT V5, Control Objectives Management Guidelines Maturity Model, DS4 Ensure Continuous Service
- PCI/DSS Security Standard V3 issued October 2008, Credit Card Security
- ITIL Version 3 Service Design Volume Section 4.5
- NFPA 1600, Standard on Disaster/Emergency Management and Business Continuity/Continuity of Operations Programs

6.	Communication methods with staff, Subcontractors, other key suppliers, and the Department when normal systems are unavailable

Each plan owner or Recovery team member communicates with their associates within a single BC plan. The ECIRT coordinates broader communications to multiple BC plans or enterprise-wide, and the Fusion Center/Humana Safety and Security team executes these communications using a notification tool. **The Kentucky Medicaid Chief Executive Officer (CEO), Jeb Duke, or a designee is the primary point of contact with the Department and other state entities.** During disaster and recovery periods, there are several lines of coordinated, purposeful communication by corporate and market-based associates, which we describe below:

The Corporate Communications team is responsible for:

- Serving as the designated primary spokesperson during any emergency event by coordinating all communications with the news media and responding to media inquiries
- Determining the information that is provided, to whom and in what format, by working with our Legal department
- Providing formal "statements" to all designated members of the IT DR teams for use if approached by the press or other new media agencies. The statement includes instructions that all associates direct all questions about the event to the Corporate Communications team for responses.
- Obtaining personnel status reports from the various recovery teams regarding injured or missing personnel to ensure no public announcements are made about these casualties before the families are notified
- Using TV, radio, and our Emergency Hotline to advise associates of alternate workplaces, defining instructions on when and where to report if mass notifications are needed
- Securing the services of a photographer to document site damages for insurance and historical purposes
- Participating as a member of the Crisis Management team

The Customer Systems Support team is responsible for:

- Providing associates, contractors, and business partners with a system status on corporate applications, systems, networks, hardware, and software infrastructure
- Assisting users when problems occur with their equipment or software, particularly if users are set up temporarily in a space other than their normal working areas
- Logging incidents in the Customer Assistance Service Desk application to track issues or problems during the recovery process. These tickets are logged with a "DR" prefix for retrieval and follow-up to resolution.

The Voice and Data Networks teams are responsible for:

- Establishing voice and data links to the alternate processing site
- Establishing the LAN/WAN/ Global Area Network connectivity for Internet/Intranet connectivity
- Re-routing Right Fax numbers as required
- Providing VOIP services at the alternate site with rerouted numbers
- Connecting local and remote users through VPNs to the alternate site

The LAN/WAN Communications team is responsible for:

- Re-establishing communications between the mainframe and the open systems and middleware servers and appliances
- Maintaining the security and integrity of the VPNs, networks, and Internet connectivity requirements

The Web Technology team is responsible for:

- Working closely with application owners, business owners, and technical teams to verify the web environment can accommodate the critical business needs with the existing tools andtechnology

The Citrix team – part of the Messaging Technology Group – is responsible for:

- Providing Citrix support so many critical applications can be accessed remotely during an emergency
- Contributing to maintaining web services uptime

The Unified Communications team is responsible for:

- Providing e-mail, fax, BlackBerry®, and instant messaging systems support
- Providing support for collaboration tools used during day-to-day operations and during any emergency

Each team manager is responsible for completing certain tasks or assigning them to team manager-alternates, who will complete tasks if the team manager is not available. These tasks include:

- Contacting the Telecom team to ensure direct call routing is functioning and providing an update on duration
- Continuing to set up periodic conference calls with all Medicaid leaders to advise of the situation
- Identifying printer/fax/copiers to use as a shared Multi-Function Device with other business areas in the recovery site

7. Testing plan

DISASTER RECOVERY PLAN

The IT Disaster Recovery Program Director is responsible for overseeing the IT DR plan's maintenance and testing. The IT DR team tests critical components and various environment combinations of those components annually. They also conduct special tests when major revisions are required to critical application environments. Where practical, the test exercises may use tabletop, walkthrough, technical, backup media restore, simulated, or automated test exercises to walk through a recovery plan.

The IT Disaster Recovery Program Manager determines and schedules test exercises that meet the desired critical testing objectives for that plan. We schedule annual testing for critical applications and systems. The list of critical testing objectives for any particular test is determined by the IT DR team, with input from the system owners and support team.

The primary objectives of testing the DR and contingency plans are to:

- Determine the effectiveness of the individual actionable technical recovery plan procedures by establishing clearly identified test objectives
- Determine the state of readiness and ability of designated individual recovery team personnel to perform assigned recovery responsibilities and to determine if cross-training of recovery personnel occurs appropriately
- Identify any gaps during the recovery process that differ from the process identified in the existing plan
- Determine whether individual team's DR plan requires updates to eliminate any gaps identified during the recovery process that might prohibit recovery within the timeframes established and accepted by the business users
- Determine whether the DR plan requires updates to reflect any changes in the business strategy, process, procedures, or technical environments

- Review how multiple teams and DR steps synchronize with recovery requirements from interrelated programs

EVALUATING DISASTER RECOVERY TEST EXERCISES

The IT Disaster Recovery Program Manager is responsible for coordinating and documenting all testing and testing results. The DR Program team facilitates and monitors testing, gathers evidence of testing documentation, identifies gaps in the existing DR plan(s) being tested, and works with the test team(s) to update plans accordingly.

Members of the IT DR team will document test results in the Executive Summary report. We provide the Executive Summary test report to executive management shortly after testing is completed and post it to the Disaster Recovery SharePoint website. An environment snapshot is added that addresses several key variables in testing, such as tester availability, upstream/downstream system identification, management support for testing, last test, data protection, technology availability, and monitoring tools, along with a prime score of no impact to production. The scorecard is divided into three areas: People, Process, and Technology (inclusive of vendor interfaces).

Follow-up focus meeting(s) are held with participating teams to discuss lessons learned and identify where specific changes must be made to the individual team plans while also providing teams with test objectives for the next test exercise.

2018 DISASTER RECOVERY EXERCISE FOR LOUISVILLE, GREEN BAY, AND HUMANA GOVERNMENT BUSINESS

Executive Summary Report, Mike Boughey, Disaster Recovery Lead, Test Dates: August 21-22, 2018

- Exercising ITI DR plans that support mainframe infrastructure recovery is an annual requirement for maintaining DR compliancy with state and federal regulations
- Validating that Humana can meet the 24-hour Recovery Time Objectives and the Recovery Point Objective of near zero data loss
- Identifying and remediating any gaps that might impede recovery during an actual disaster event

EXERCISE SUMMARY

The annual Corporate Mainframe Disaster Recovery Exercise was successfully completed on August 21-22, 2018. The test scope involved recovery of the data and functionality for all mainframe applications supporting Corporate Humana and Humana Government Business (HGB) using the alternate data center in Simpsonville.

The exercise began at 8:28 a.m. on August 21, when the DR team initiated use of Humana's notification tool (Send Word Now) to alert ITI and PSM managers of the start of the exercise. Teams were instructed to dial in to a central bridge to receive additional information. Managers were on the call by 8:35 a.m. and within five minutes, the Storage team had stopped replication. Recovery of the test infrastructure began. Mainframe recovery and checkout completed at 5:30 p.m., at which time the system was turned over to PSM and business teams for data validation and system functionality testing. The DR team recorded that it completed successful recovery nine hours after the initial alert. The "ITI Recovery Overview" contains chronologic recovery details.

Recovery Time – 9 hrs.
(Initial alert - mainframe recovery and checkout complete)

MAINTAINING CORPORATE IT DISASTER RECOVERY PLAN

The IT Disaster Recovery Program Director is responsible for maintaining this umbrella IT DR Plan in a current and ready state. The factors driving plan maintenance are:

- Major technical changes to the data center environment
- Test exercises revealing vulnerabilities or gaps in individual team recovery plans
- Plan strategies that change significantly
- Major corporate re-organizations
- Changes in disaster recovery and resiliency strategies

Humana reviews and updates this umbrella plan as needed.

AUDITING CORPORATE IT DISASTER RECOVERY PLAN

The Internal Audit Consulting Group (IACG) reviews the corporate IT DR plan. The audit provides an objective third-party check of the plan's value. IACG is particularly important because external customers and vendors depend on the corporate DR plan functionality.

Periodically, external auditors review company disaster recovery processes to provide an independent assessment of the DR program. External audits identify gaps or processes that might raise the enterprise disaster recovery maturity level. We use the identified gaps as input for plan revision and testing with the next test cycle and to improve processes and procedures involving DR planning and testing across various other corporate functions.

BUSINESS CONTINUITY

Humana requires business areas to exercise BC plans annually. We determine the type of exercise performed by the criticality of the business process, which is the result of the business impact analyses. Those processes that must be restored within zero to 48 hours are deemed critical functions, which we must test annually. We also document and resolve any lessons learned based on the business tolerance to disruptions.