| **CO** |  | **Control Objective** | **XXXXX Control** | **Test Step** | **Issue if control not in place** | **Workpaper Reference** | **Test Result** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Governance** | GV01 | The organization’s leadership understands the current Information System Continuity Plan (ISCP) risk level and impact. |  | **Inquiry and Observation:** Verify Management is briefed a minimum of annually on the ISCP/DRP. Inspect meeting minutes or sign-offs for evidence of review. | Yes | E5-1 |  |
| GV02 | Sufficient resources, people, and budgeted funds have been allocated to prepare, maintain, and test the ISCP. |  | **Inquiry and Observation**: Verify DRP maintenance and TT&E is included in the annual budget. | Yes | DR01 |  |
| GV03 | A central group has been created within the organization that is responsible for ISCP governance, coordination, consulting, and training. |  | **Inquiry and Observation:** Verify a Management team has been assembled to oversee the ISCP Plan. Inspect a list of team members and verify the following:   * Members of senior management are included on the team * All team members are current employees * Inspect evidence of team meetings (meeting planners, meeting minutes) | Yes | DR01 | each business unit. |
| GV04 | The ISCP team leader(s) is qualified to perform his or her job functions. The following certifications or alternate training/certifications have been obtained and maintained.   * Certified Business Continuity Professional (CBCP) * DRI International Certification (DRII) |  | **Inquiry:** Identify the key personnel responsible for maintaining the ISCP plan, ISCP coordination, ISP training, and ISCP testing. Review their qualification and assess for reasonableness. | No, certifications are a best practice recommendation. | E5-1 |  |
| GV05 | A data inventory is available of all data stored on systems, as well as their criticality and security classifications. |  | **Observation:** Inspect the data inventory and verify it is sufficiently detailed (application, description, DR classification, security classification, risk assessment rating).  Verify the data inventory has been updated within the last 12 months. | Yes | GV05 |  |
| GV06 | A device inventory is maintained. Infrastructure components are assigned criticality ratings based on the applications they support. |  | **Observation:** Inspect the device inventory and verify it is sufficiently detailed (device name, type, application, location, and owner).  Verify the device inventory was updated within the last 12 months. | Yes | N/A |  |
| GV07 | IT scanning tools are in place to identify new devices on the network. Scans are periodically performed to update the software and device inventory. |  | **Inquiry:** Determine procedures for identifying new applications and devices and periodically updating the inventory. | No, procedures need to be in place- does not necessarily need to be an automated scan. | N/A |  |
|  | GV08 | An IT risk assessment is conducted and updated annually, identifying vulnerabilities, threats, and risks for all systems identified on the inventory. |  | **Observation and Testing:** Inspect a copy of the latest IT risk assessment and verify it has been performed with the last 12 months.  Compare to application inventory to validate its completeness. | Yes | DR01 |  |
|  | GV09 | The Physical Risk Assessment is made for each critical application, including the following components:   * Location of Servers (secure data center, office) * Redundancy of network components (secure data center, office) * Fire suppression systems (secure data center, office) * HVAC systems * Redundancy of power sources * Water prevention and detection * Alarms, security cameras and surveillance * Secure storage of backup media and disks (secure data center, office, off-site location) * Condition and maintenance of facility |  | **Observation and Testing:** Inspect a copy of the latest Physical risk assessment and verify it has been performed with the last 12 months.  Compare to the device inventory for a sample of critical applications to validate its completeness. | No- this is a best practice recommendation only. This may be covered in the IT risk assessment process. | DR01 |  |
|  | GV10 | The Management Disaster Awareness Assessment is made for each critical application and includes the following components:   * Delegation of authority, succession planning list is in place for application support * End users are aware of who to contact in the event of an outage or disaster. * First responders are aware of what they are supposed to do and when they are supposed to do it. * End users and first responders have a contact list of management that can be reached 24X7. * Support personnel are aware of where the system backups are and how to retrieve them. * Support personnel have infrastructure specifications and are aware of where to procure equipment from when necessary. |  | **Inquiry and Testing:** Determine if a formal Management Disaster Awareness Assessment was completed.  Select a sample of ISCP/DRP contacts for critical applications and interview them. Determine if the attributes in the control objective column are met. | No- this is a best practice recommendation only. This may be covered in the TT&E (Training, testing, and exercise) process. Assess results of the test to determine if an issue is warranted. | DR01 |  |

| **Business Impact Analysis (BIA)** |  | **Control Objective** | **XXXX Control** | **Test Step** | **Issue if control not in place** | **Workpaper Reference** | **Test Result** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| BI01 | A Business Impact Analysis (BIA) is prepared to identify business processes that are integral to keeping the business unit functioning in a disaster. |  | **Observation and Testing:** Inspect the current Business Impact Analysis and verify the following:   * The BIA was updated within the last 12 months. * Compare the BIA to the software inventory to verify completeness. | Yes | BI02a-f |  |
| BI02 | The following objectives are documented on the BIA for all critical information systems:  MTD- Maximum Tolerable Downtime  RTO- Recovery Time Objective (targeted time to return system operations after outage)  RPO- Recovery Point Objective (acceptable post restore data loss-minutes, hours, days, weeks)  SRT- System Recovery Time (estimated time to recover operations after an outage) |  | **Observation:** Inspect the current Business Impact Analysis and verify all objectives noted were documented in the analysis for each system listed. | Yes | BI2a-f |  |
| BI03 | Dollar totals are computed on the BIA, representing the estimated loss for every minute/hour/day a system is down. Estimates include the following components:   * Hard Loss (cost of equipment, software) * External Customers (lost orders) * Internal Customers * Operating Expense (downtime) * SLA impact * Legal impact * Dependent function loss * Business partner functions * Reputational Loss |  | **Observation and Walk through:** Inspect the current Business Impact Analysis and verify dollar total estimates for downtime were documented on the BIA.  Select one BIA outage cost estimate and walk through the process for developing that estimate. Interview staff that prepared the estimate and inspect documentation supporting the estimate. | Yes | BI2a-f |  |
| BI04 | The IT Risk Assessment, Physical Assessment, and Management Disaster Awareness Assessment ratings are included as components of the BIA Risk Assessment. |  | **Observation and Walk through:**  Inspect the current Business Impact Analysis and verify a risk rating has been assigned to each system.  Select one system on the BIA and walk through the process for developing the risk rating. Inspect the reports and documentation supporting the risk rating. | No, risk rating should be assigned to systems and control gaps should be noted in the report. Determine process for determining risk ratings and assess its adequacy. | DR01 |  |
| BI05 | The BIA summary report includes the following components:   * Management Summary and Background * Project scope and assumptions * Project objectives * Risk assessment objectives * Project actions that were completed * List of findings (threats, consequences, mitigating factors, likelihood, and impact) * Existing strengths and problem areas * Budget to address problem areas * Summary of insurance coverage   Final analysis and recommendations. |  | **Observation:**  Inspect the BIA management summary and verify the following:  -the report was issued within the last 12 months.  -the components noted were included in the report  -the report was distributed to senior management | Yes | DR01 |  |
|  |  |  |  |  |  |  |

| **Resiliency and Mitigation Strategies** |  | **Control Objective** | **Laclede Control** | **Test Step** | **Issue if control not in place** | **Workpaper Ref** | **Test Results** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| MT01 | Dual power supplies, UPS units, and generators are in place on critical hardware to mitigate the risk from power outages. | Per questionnaire, this is in place. | **Inquiry:** Select a sample of critical systems from the BIA. Per inquiry, determine if the control is in place. | Yes | E5-1 | Per Questionnaire, control is in place. |
| MT02 | Backup media are stored offsite or at alternative sites. | Per questionnaire, this is in place. | **Inquiry:** Select a sample of critical systems from the BIA. Per inquiry, determine if the control is in place. | Yes | E5-1 | Per Questionnaire, control is in place. |
| MT03 | Hardware, software, and peripheral configurations are standardized across the organization. | Per questionnaire, this is in place. | **Inquiry:** Select a sample of critical systems from the BIA. Per inquiry, determine if the control is in place. | Yes | E5-1 | Per Questionnaire, control is in place. |
| MT04 | Backups of file share servers, PC’s and peripherals connected to the network are automated. | Per questionnaire, this is in place. | **Inquiry:** Select a sample of critical systems from the BIA. Per inquiry, determine if the control is in place. | Yes | E5-1 | Per Questionnaire, control is in place. |
| MT05 | Threats to the LAN, WAN, and telecommunications systems and points of failure are identified in the BIA and appropriate mitigation is applied, such as:   * Redundant cables * Redundant network components (routers, switches, firewalls) or onsite spares. * Redundant communication links (T-1 connection) * Redundant network service providers (NSP) or internet service providers (ISP) | Fully meshed redundant network exists with multiple WAN paths to the data center. | **Inquiry:** Select a sample of sites from the BIA. Per inquiry, determine if the control is in place. | Yes | E5-1 | Per Questionnaire, control is in place. |

| **Resiliency and Mitigation Strategies** |  | **Control Objective** | **Laclede Control** | **Test Step** | **Issue if control not in place** | **Workpaper Ref** | **Test Results** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| MT06 | If remote access is identified as a contingency strategy, data bandwidth requirements are identified and a scalable solution and contingency strategy is developed. | Yes. Capacity can be increased. | **Inquiry and Observation:** Determine if remote access is a DR solution.  Review the ISCP/DRP and verify procedures are in place for scaling up/down the remote access systems.  Inspect capacity planning documentation for the remote access system and verify the following:   * Capacity plans have been updated within the last 12 months. * Capacity plans include capacity requirements based on a variety of DR events (weather, site outage, etc.) | Yes | E5-1 | This step will be performed in a subsequent review. Testing was not performed due to general absence of controls. |
| MT07 | Recovery solutions and sites have been identified for all critical systems:   * Hot recovery * Warm recovery * Cold recovery * No recovery | Backup and recovery capabilities have not been identified for all critical systems identified in the DRP. General recovery and replication strategies are detailed in Section 10.0.  Management’s questionnaire answer for all systems:  *Cold site using replicated data. We do not use tapes.* | **Inquiry and Test:** For a sample of critical systems on the BIA, determine the recovery solutions and assess the appropriateness based on the criticality rating on the BIA. | Yes | DR01 | **Exception Noted:** Backup and recovery capabilities have not been identified for critical systems in the DRP. Backup and Recovery capabilities must be identified to determine if system RTO and RPO’s can be met. |

| **Resiliency and Mitigation Strategies** |  | **Control Objective** | **Laclede Control** | **Test Step** | **Issue if control not in place** | **Workpaper Ref** | **Test Results** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| MT08 | Backup/recovery strategies are reasonable based on the system impact level/criticality. See examples below:   * LOW- tape backup: relocate to cold site * MODERATE- optical backup, WAN/VLAN replication: relocate to warm site * HIGH- mirror systems or disc replication: relocate to hot site | See above- it appears as though all systems replicated to cold site. | **Testing:** For a sample of critical systems on the BIA, inspect the DRP to validate specific guidelines are in place for retrieving and restoring systems at recovery sites. | Yes | DR01 | See MT07 |
| MT09 | Local PC backup procedures are in place and have been effectively communicated to employees (i.e. where to and where not to store critical files on their devices). | Per questionnaire, this is in place. | **Inquiry and Observation:** Inquire as to procedures for storing information on local PC’s and inspect the policy that documents procedures. |  | E5-1 | See MT07 |
| MT10 | Data backup policies specify minimum frequency and scope of backups based on data criticality and frequency that new information is introduced. | Per questionnaire, this is in place. | **Observation:** Inspect backup policies to determine if guidelines for developing backup strategies are provided based on the RPO, RPT, SRT, and MTD objectives. |  | E5-1 | See MT07 |
| MT11 | Backup schedules are reasonable based on RPO’s (Recovery Point Objectives) noted in the BIA. | Backup and recovery capabilities have not been identified for all critical systems identified in the DRP. General recovery and replication strategies are detailed in Section 10.0. | **Testing:** For a sample of critical systems on the BIA, obtain the backup schedule and assess the reasonableness based on the RPO, RPT, SRT, and MTD objectives. |  | DR01 | See MT07 |

|  |  | **Control Objective** | **Laclede Control** | **Test Step** | **Issue if control not in place** | **Workpaper Ref** | **Test Results** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Vendor Management** | VM01 | Emergency and crisis centers have been established and equipped. | Alternative Work locations (Section 11.1) have not been identified in the draft DRP.  Per Questionnaire, no emergency or disaster scenarios were identified. | **Inquiry and Observation:** Inspect the ISCP/DRP documentation and determine if emergency or crisis centers have been identified.  Inquire as to the procedures for the following:   * Management of these organizations * Communication To (periodic meetings, distribution of DRP plans) * Communication From (vendor notification of significant changes in their operations and capacity). * Oversight and performance management (SLA reports, vendor evaluations) * Inventories and accounting for equipment held by off-site service providers. | Yes | DR01 | **Exception Noted:** Alternate work locations were not identified in the DRP draft. Alternative work locations should be established and equipped. Additionally, providers should be actively managed to ensure the following:   * Operation and capacity requirements are defined in the written agreement. * Facilities are routinely inspected to ensure requirements can be satisfied. * Laclede equipment stored and managed by providers are periodically inventoried and inspected. |

|  |  | **Control Objective** | **Laclede Control** | **Test Step** | **Issue if control not in place** | **Workpaper Reference** | **Test Results** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Vendor Management** | VM02 | Formal contracts and SLA’s are in place for alternate site providers. Contacts include the following attributes:   * Contract/agreement duration * Cost/fee structure for disaster declaration and occupancy (daily usage), administration, maintenance, testing, annual cost/fee increases, transportation support codes, billing and payment schedules * Disaster declaration (i.e. circumstances constituting a disaster, notification procedures) * Site/facility priority access and/or use * Site availability * Site guarantee * Other clients subscribing to the same resources, total number of subscribers * Contract/agreement modification specifications * Contract/agreement termination conditions * Process to negotiate extension of service * Guarantee of compatibility * Information system requirements * Change management and notification requirements * Security requirements * Staff support to be provided * Facility services to be provided * Testing, schedules, availability, test time duration * Records management (tapes and records) * Service level management and performance measure * Work space requirements * Supplies to be provided | BSW will forego testing of DR provider contracts since DRP plan is still in progress. | **Testing:** Select a sample of DR service providers. Inspect contacts to verify (1) contracts are in place (2) Agreements are current (3) Attributes identified in the control objective are in place | Yes- if contracts not in place.  No- if some attributes are not present. | N/A | This step will be performed in a subsequent review. Testing was not performed due to general absence of controls. |

|  |  | **Control Objective** | **Laclede Control** | **Test Step** | **Issue if control not in place** | **Workpaper Reference** | **Test Results** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | VM03 | DR plan documentation has been distributed to key personnel and contractors. | The DR plan is still in draft form and has not been distributed. | **Inquiry:** Determine procedures for distributing and training vendors on the ISCP/DRP plan. | Yes | DR01 | This step will be performed in a subsequent review. Testing was not performed due to general absence of controls. |

| **CO** |  | **Control Objective** | **Laclede Control** | **Test Step** | **Issue if control not in place** | **Workpaper Ref** | **Test Results** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Disaster Recovery Plan** | DR01 | A formal disaster recovery (DR) and information security continuity strategy has been developed addressing the actual steps, people, and resources required to recover each critical business process. | The DR plan is in draft and approximately 30% complete. List of critical systems, metrics, key personnel, communication plans, etc. are incomplete and detailed steps for recovering systems have not been developed. | **Observation:** Inspect a copy of the ISCP/DRP and verify the document is current, and at a high level, includes all required elements. | **Yes** | **DR01** | **Exception Noted:** Include information in background section of the report. |
| DR02 | Systems supporting critical business functions identified on the BIA are included in the ISCP/DRP, as well as hardware, software, and personnel supporting those systems. | BIA surveys were distributed to business units for completion. Business owners identified critical systems in their surveys, but system infrastructure and resources have not been identified. | **Testing:** For a sample of systems included on the BIA, inspect the ISCP/DRP to verify all system components are identified and recovery plans are in place for those components. | **Yes** | **DR01** | See GV06 |
| DR03 | The following common platform types are taken into account in the DR plan:   * Client/server systems * Telecommunication systems * Mainframe systems | A high level diagram of servers and backup systems included in Section 9.2 of the DRP. Section 8.3 was reserved for Network architecture diagrams. These were not in place. | **Observation:** Inspect a copy of the ISCP/DRP and verify, at a high level, plans are developed for various types of systems. | **Yes** | **DR01** | See GV06 |
| DR04 | The sequence of system recoveries reflect the system’s MTD (Maximum Tolerable Downtime).  Recovery plans specify the order of recovery in both short-term and long-term timeframes | A high level sequence of recovery operations was detailed in Section 6.1. Basically, the LAN functionality is returned first, followed by WAN, followed by the internet, then tier1, tier2, and tier 3 applications.  The specific order of Tier 1, Tier 2, and Tier 3 applications was not specified in the draft DR plan, as well as interdependencies and prerequisites for restoring critical applications. | **Observation:** Inspect the ISCP/DRP and, at a high level, determine if the sequence of system(s) to be restored in a full-scale disaster scenario. | **Yes** | **DR01** | **Exception Noted:**  The sequence of system recovery operations, detailing the explicit order of recovery for each application and major infrastructure components was not specified in the draft DRP. |

| **CO** |  | **Control Objective** | **Laclede Control** | **Test Step** | **Issue if control not in place** | **Workpaper Reference** | **Test Results** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Disaster Recovery Plan** | DR05 | The ISCP/DRP contains the following components:   * Personnel Contact List * Vendor Contact List * Detailed Recovery Procedures * Alternate Processing Procedures * System Validation Checklist * Diagrams (System input/output) * Interconnections Table (Interface Workflow) * Test and Maintenance Schedule * Plan Change Log * The BIA grid * Equipment and system requirements list of the hardware, software, firmware, and other resources. * Vendor SLAs, reciprocal agreements, and other vital records | None of the items listed to the left were included in the draft DRP. | **Observation:** Inspect the ISCP/DRP and review for the components listed. | **Yes** | **DR01** | **Exception Noted:**  The Draft DRP does not contain the following components:   * Personnel Contact List * Vendor Contact List * Detailed Recovery Procedures * Alternate Processing Procedures * System Validation Checklist * Diagrams (System input/output) * Interconnections Table (Interface Workflow) * Test and Maintenance Schedule * Plan Change Log * The BIA grid * Equipment and system requirements list of the hardware, software, firmware, and other resources. * Vendor SLAs, reciprocal agreements, and other vital records |

| **CO** |  | **Control Objective** | **Laclede Control** | **Test Step** | **Issue if control not in place** | **Workpaper Reference** | **Test Results** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Disaster Recovery Plan** | DR06 | Teams have been assembled to implement the DR strategy, including the following:   * Management team * Outage assessment team * Operating system administration team * Server recovery team * LAN/WAN recovery team * Database recovery team * Network operations recovery team * Application recovery team * Telecommunications team * Test team * Transportation and relocation team * Media relations team * Legal affairs team * Physical/personnel security team * Procurement team (equipment and supplies)   Teams are sufficient in size to remain viable if some members are unavailable. | Section 3.0 identifies the following POCs:   1. Crisis Management Team (included several contacts from various functions- Executives, Legal, HR, Finance, etc.) 2. ITS recovery team    1. One contact for infrastructure    2. One contact for applications and databases    3. One contact for telecommunications    4. One contact for customer service    5. Once contact for SCADA/Industrial Control   Contacts for specific applications and infrastructure components were not identified. Additionally, backup contacts or escalation plans were not identified. Phone numbers or after-hours contact information was not provided.  Vendors were identified, but contact names and numbers were not included. Also, vendors were in broad categories (Oracle for databases, VMWare for virtualization, Cisco for network components). | **Observation:** Inspect the ISCP/DRP and verify teams have been assigned to implement the DR strategy. Verify teams have sufficient numbers of members.  **Testing:** Select a sample of team rosters. Verify the personnel assigned to those teams are current employees/contractors. |  | **DR01** | **Exception Noted:**  The Draft DRP denoted Crisis Management team and ITS recovery team contacts, but the following information was not present:   * After hours contact information * Escalation plans and backup contacts. * Contacts for specific applications and infrastructure components were not identified. Examples include LAN/WAN, database, network operations, application, relocation, procurement team contacts. * Vendor contact names, purposes, procurement instructions. |
| DR07 | Team leaders have been identified to lead each team, act as each team’s representative to management, and confer with other team leaders. | Individual recovery teams, team leaders, and points of contacts were not identified in the DRP draft. | **Observation:** Inspect a roster of DR teams and verify leaders have been appointed to each team. |  | **DR01** | **Exception Noted:** Individual recovery teams, team leaders, and point of contacts were not identified in the DRP draft. |

| **CO** |  | **Control Objective** | **Laclede Control** | **Test Step** | **Issue if control not in place** | **Workpaper Reference** | **Test Results** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Disaster Recovery Plan** | DR08 | DR team members are geographically disbursed. Alternates are trained or teams are cross-trained to handle duties. |  | **Observation:** Inspect the roster of DR teams and team members and verify they are geographically disbursed.  **Testing:** Select a sample of team leaders, determine if succession plans are in place to stand in for team leaders if they are not available. |  | **DR01** | This step will be performed in a subsequent review. Testing was not performed due to general absence of controls. |
| DR09 | Strategies are in place for replacing equipment, including , but not limited to the following:   * Procurement plans * Equipment inventory (an inventory of spares is maintained at an offsite location) * Hot site reciprocal agreements (may be jointly owned or rented from hot site) | Equipment replacement procedures were not detailed in the Draft DRP. | **Observation:** Inspect the ISCP/DRP and determine if procedures for replacing equipment are documented in the plan. | **Yes** | **DR01** | **Exception Noted:** Procedures and points of contact for replacing equipment were not detailed in the draft DRP plan. |
| DR10 | DRP documentation has been distributed to key personnel and contractors. | The DRP is still in draft form and is not ready for distribution. | **Inquiry:** Determine procedures for communicating and distributing the plan. | **Yes** | **DR01** | This step will be performed in a subsequent review. Testing was not performed due to general absence of controls. |
| DR11 | A Master Scenario Events List (MSEL) is prepared listing the event description and the expected results. | 5.2.4 Risk Assessment Score Card is present in the DRP, but probability ratings, impact ratings, consequences, and remedial actions fields have not been populated. | **Observation:** Inspect the ISCP/DRP document for a MSEL. | **No** | **DR01** | **Exception Noted:**  A Master Scenario Events List (MSEL) is present in the DRP, but has not been populated. Remedial actions for common disasters are not detailed in the plan. |
| DR12 | Activation criteria is developed and documented in the DRP. Criteria may be based on:   * Extent of any damage * Criticality of the affected systems * Expected duration of the outage lasting longer that the RTO. | 10.5 Provides general criteria for declaring a disaster. Basically, if the data center is destroyed or non-operational for more than 2 days, a disaster is declared. All other incidents are referred to the Management Team. Management Team POC’s are not specified (unless Crisis Management team). | **Observation:**  Inspect the ISCP/DRP for Plan Activation criteria and procedures. | **Yes** | **DR01** | **Exception Noted:** Detailed activation criteria for declaring a disaster are not documented in the draft DRP. Section 10.5 advises that the Management team will perform the assessment, however, first responder contact instructions, as well as triggers for alerting the Management team have not been documented in the DRP. |

| **CO** |  | **Control Objective** | **Laclede Control** | **Test Step** | **Issue if control not in place** | **Workpaper Reference** | **Test Results** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Disaster Recovery Plan** | DR13 | Notification Procedures have been documented in the DRP. Procedures describe method used to notify recovery personnel during business and non-business hours. Contingency plans should be in place when the automatic notification system or email is down. | Section 12.1 Communications Plan is blank in the DRP Draft. | **Observation:** Inspect the ISCP/DRP for Notification Procedures. Verify contingency plans have been documented in case the standard notification method is not available. | **Yes** | **DR01** | **Exception Noted:** The detailed communications plan (Section 12.1) has not been developed in the Draft DRP. |
| DR14 | An “Outage Assessment Team” has been designated and receives first notice of a system disruption or outage. Criteria for assessing the outage have been documented in the DRP. The following areas, at a minimum, have been addressed:   * Cause of outage * Potential downstream disruptions or damage * Status of physical infrastructure * Inventory of system equipment and functional status * Type of damage to equipment or data * Inventory of items to be replaced   Estimated time to restore operations. | A Crisis Management Team (3.3) has been designated. Criteria for assessing the outage have NOT been documented in the DRP (see DR12). Additionally, criteria for alerting the Crisis Management Team, as well as first responder contact information is not detailed in the draft DRP. | **Observation:** Inspect the ISCP/DRP for evidence that an Outage Assessment Team is in place, such as notification procedures and contacts. |  | **DR01** | **See DR12** |

| **CO** |  | **Control Objective** | **Laclede Control** | **Test Step** | **Issue if control not in place** | **Workpaper Reference** | **Test Results** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Disaster Recovery Plan** | DR15 | The DRP recovery phase documentation provides general procedures for restoring information system and components. The following tasks are delegated to appropriate teams:   * Obtaining authorization to access damaged facilities * Notifying internal and external business partners * Obtaining necessary office supplies and work space * Obtaining and installing necessary hardware components * Obtaining and loading backup media * Restoring critical operation system and application software * Restoring system data to a known state * Testing system functionality including security controls * Connecting system to network or other external systems * Operating alternate equipment successfully | None of the items to the left are detailed in the draft DRP.  Are individual plans in place for various applications? | **Testing:** For a sample of critical systems on the BIA, determine if specific recovery procedures are documented. Walk-through procedures and assess the completeness. | **Yes** | **DR01** | **Exception Noted:** DRP appendices do not included detailed recovery procedures for critical systems. Such procedures include, but are not limited to the following:   * Obtaining authorization to access damaged facilities * Notifying internal and external business partners * Obtaining necessary office supplies and work space * Obtaining and installing necessary hardware components * Obtaining and loading backup media * Restoring critical operation system and application software * Restoring system data to a known state * Testing system functionality including security controls * Connecting system to network or other external systems * Operating alternate equipment successfully |
| DR16 | Reconstitution phase activities are documented in the DRP. Primary activities for validating successful recovery and deactivation of the plan. Specific procedures for validating each system are documented in that system’s recovery procedures. | Reconstitution procedures are not detailed in the Draft DRP. | **Testing:** For a sample of critical systems identified in the BIA, verify procedures have been documented for testing/validating the system post-recovery. | **Yes** | **DR01** | **Exception noted:**  Reconstitution procedures to validating successful recovery and releasing systems to users have not been documented for critical applications. |
| DR17 | Procedures are in place for obtaining a new data backup of the system once operational, in addition to returning retrieved backup or installation media. | Post-restore backup procedures are not in place. | **Testing:** For a sample of critical systems identified in the BIA, verify procedures are in place for obtaining backups post-recovery and returning backup media. | **Yes** | **DR01** | **Exception noted:**  Procedures for obtaining new data backups and monitoring recovered systems have not been documented for critical applications. |

| **CO** |  | **Control Objective** | **Laclede Control** | **Test Step** | **Issue if control not in place** | **Workpaper Reference** | **Test Results** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Disaster Recovery Plan** | DR18 | The DRP plan reviews are performed at an organization-defined frequency or whenever significant organizational or system changes occur. At a minimum, plan reviews focus on the following:   * Operational requirements * Security requirements * Technical procedures * Hardware, software, and other equipment (types, specifications, and amount) * Names and contact information of team members. * Names and contact information of vendors, including alternate and office vendor POC’s. * Alternate and offsite facility requirements * Vital records | Not applicable at this juncture. DRP is still in draft phase. | **Observation:** Verify the ISCP/DRP plan documents the maintenance schedule and maintenance procedures. Affirm the elements noted appear in the maintenance procedures. | **Yes** | **DR01** | This step will be performed in a subsequent review. Testing was not performed due to general absence of controls. |

| **CO** |  | **Control Objective** | **Laclede Control** | **Test Step** | **Issue if control not in place** | **Workpaper Reference** | **Test Results** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Data Security** | **DS01** | The DR plan outlines perimeter defense requirements and configurations to bring each system’s security up to pre-disaster state. | Control not outlined in DRP | **Testing:** For a sample of systems, verify perimeter defense and security requirements are specified in system recovery and validation procedures. |  | **DR01** | **Exception Noted:** Perimeter defense requirements for bringing each system’s security up to pre-disaster state have are not defined in the draft DR plan. Such procedures include:   * Reinstallation of configuration of firewalls and security tools (IDS/IPS). * Restoration of host system images and checklists to validate secure configuration of servers. * Running vulnerability scans on systems. |
| **DS02** | Procedures are in place to reinstall and configure firewalls and perimeter security tools (IDS/IPS) on the network perimeters and systems connecting to the web. | Control not outlined in DRP | **Observation:** Inspect network recovery procedures and verify procedures are in place for reinstalling the firewall, IDS, IPS, and other network perimeter tools. |  | **DR01** | **See DS01** |
| **DS03** | Host system images are maintained with the most current security configurations. DR Procedures are in place to update patches prior to bringing systems back online. | Control not outlined in DRP | **Testing:** For a sample of systems, verify DR procedures require the system components to be brought up to the most current security patch level. |  | **DR01** | **See DS01** |
| **DS04** | DR procedures require systems to be scanned for significant security vulnerabilities prior to bringing systems back online. | Control not outlined in DRP | **Testing:** For a sample of systems, verify DR procedures require servers, databases, and web-facing application be scanned for security vulnerabilities prior to bring systems back online. |  | **DR01** | **See DS01** |
| **DS05** | Media readers are available at alternate recovery site to read encrypted media. Key management procedures are in place for securing and retrieving keys. Keys are stored separately from the encrypted media. | Control not outlined in DRP | **Observation:** Inspect backup and recovery procedures and verify encryption key management procedures are in place. |  | **DR01** | This step will be performed in a subsequent review. Testing was not performed due to general absence of controls. |

| **CO** |  | **Control Objective** | **Laclede Control** | **Test Step** | **Issue if control not in place** | **Workpaper Reference** | **Test Results** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Test, Training, and Exercise Plan (TTE)** | TT01 | A formal Test, Training, and Exercise (TTE) plan is developed and contains the following components:   * Purpose * Effective Date * Objectives * Applicability and scope * Roles and responsibilities of key business units and staff positions * Resource requirements * Management review and approval * Points of contact * Overall schedule * Event Methodology (topic, scope, and schedule) | Section 4.6 states the following: At a minimum, this BC&DR plan will be exercised twice annually, once as a tabletop evaluation of processes, and one for full execution. Exercising the plan in this manner will ensure ITS personnel are familiar with their assignments and confident in their capabilities. After each exercise, lessons learned will be captured and recommendations for changes will be submitted to the Vice President, Information Technology Services for review and inclusion within the plan.  A formal test plan and schedule has not yet been developed. | **Observation:** Inspect the TTE plan for the components listed in the objective. |  | **DR01** | **Exception:** Although basic testing and evaluation requirements have been established within the plan, a formal test plan and schedule has not yet been developed. Testing methodologies and strategies will be defined in Phase 3. The test plan will be implemented in Phase 4. |
| TT02 | A DR Plan Coordinator has been designated to develop the TTE plan and coordinate events. | The DRP Coordinator had left the Company at the time of our review and no replacement was designated. | **Inquiry:** Determine if a DR Plan Coordinator has been designated. Inspect the documented job description responsibilities if available. |  | DR01 | See TT01 |
| TT03 | A formal TTE schedule is developed. The following are included:   * Tabletop exercises for low-impact systems * Functional exercises for moderate-impact systems * Full scale functional exercises for high-impact systems * Training exercises are scheduled for various DR teams | A TTE plan has not been developed. | **Observation:** Inspect the ISCP/DRP formal test schedule and determine that regular “tests” are schedule and adequate coverage is obtained. |  | DR01 | See TT01 |

| **CO** |  | **Control Objective** | **Laclede Control** | **Test Step** | **Issue if control not in place** | **Workpaper Reference** | **Test Results** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Testing, Training, and Exercise Plan** | TT04 | Tabletop exercises are performed periodically, or following organizational changes or significant updates to the DR plan. Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. | Control not present | **Testing:** Inspect documentation of tabletop exercises performed over the last three years. |  | DR01 | See TT01 |
| TT05 | Functional exercises are periodically performed in a simulated operational environment to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects to the DR plan. | Control not present | **Testing:** Inspect documentation of functional exercises performed over the last three years. |  | DR01 | See TT01 |
| TT06 | Full-scale functional exercises are periodically performed to simulate full recovery and reconstitution of system operations at an alternate facility. | Control not present | **Testing:** Inspect documentation of full-scale functional exercises performed over the last three years. |  | DR01 | See TT01 |
| TT07 | A formal event report is prepared, recapping tests or activities performed, identifying problems and proposed solutions, as well as providing specifications for follow up testing or training. | Control not present | **Testing:** Inspect formal reports for all exercises performed over the last 3 years. |  | DR01 | See TT01 |
| TT08 | Relevant training programs for each team dependent upon task, including crisis communications/ media training have been developed. | Control not present | **Testing:** For a sample of systems, determine if application team members participated in training exercises over the last 3 years (source: test plans, reports, inquiry) |  | DR01 | See TT01 |
|  |  |  |  |  |  |  |  |