
Roberta J. Witty

Identity and access management (IAM) and business continuity management (BCM) are key components of IT governance risk and compliance (IT GRC), and they intersect at four points in each program — IT service risk profiling, role life cycle management, access policy violations, and provisioning and access management for recovery operations. Activities for each area need to be included in IAM and BCM planning programs.

Key Findings

• Not having the needed access to mission-critical systems and recovery procedures during a recovery effort can delay the business coming back online.

• Few IAM programs include recovery access requirements in their development processes and ongoing maintenance activities. BCM programs tend to include access requirements more often.

• Recovery access requirements must be managed for all workforce members, regardless of their role in the recovery process.

• Granting emergency recovery access in the midst of a disaster can create access policy violations that may not get closed after the situation returns to business as usual, thereby creating potential exposures of confidentiality, integrity and privacy to organizational information.

Recommendations

• Establish BCM and IAM as key IT GRC activities.

• Jointly manage recovery access requirements in IAM and BCM programs. Leaving out one side of the equation means that the requirements might be out-of-date when most needed — when disaster strikes.

• Establish planned recovery and emergency recovery access request processes, roles and workflows that meet the needs of the IAM and BCM requirements.

• After the disaster stand-down, roll back recovery access entitlements provisioned during the disaster, and perform an access certification/attestation to ensure that they have been correctly deprovisioned, thereby closing any access policy violations that might have occurred during recovery.
TABLE OF CONTENTS

Analysis ............................................................................................................................................. 3
1.0 Best Practices for Recovery and BAU Access Requirement Alignment ................................. 4
  1.1 Best Practice No. 1: IT Service Risk Profiling — Classify Your Business Processes and IT Services........................................................................................................... 4
  1.2 Best Practice No. 2: Role Life Cycle Management — Develop Recovery Team Roles and Responsibilities .......................................................................................................................... 7
  1.3 Best Practice No. 3: Role Life Cycle Management — Build Recovery Access Requirements into Existing Roles ................................................................................................. 8
  1.4 Best Practice No. 4: Managing Access Policy Violations During a Disaster ... 10
  1.5 Best Practice No. 5: Recovery Operations — Establish Emergency Recovery Access Request Workflows ................................................................................................................. 12
  1.6 Best Practice No. 6: Recovery Operations — Establish Alternative Authentication Methods.................................................................................................................................. 12
  1.7 Best Practice No. 7: Recovery Operations — Provision Essential Nonelectronic Resources ........................................................................................................................................ 13
  1.8 Best Practice No. 8: Recovery Operations — Disaster Stand-Down: Deprovision Access Changes Made During the Disaster .................................................................................. 14
2.0 Tactical Guidelines ...................................................................................................................... 14

Recommended Reading .................................................................................................................. 14

LIST OF TABLES

Table 1. Manufacturing Firm IT Service Risk Profiling ........................................................................ 6

LIST OF FIGURES

Figure 1. Where IAM and BCM Intersect ......................................................................................... 3
Figure 2. IT Service Risk Profiling for Business Continuity Management ........................................ 5
Figure 3. Application Risk Profiling .................................................................................................. 6
Figure 4. Recovery Team Identification ............................................................................................ 8
Figure 5. Disaster-Time Activity Types ............................................................................................. 9
Figure 6. Potential Access Policy Violations Due to Reduced Workforce ......................................... 11
Figure 7. Summary of Recovery Activities and Recovery Access Requirements .............................. 12
ANALYSIS

During a crisis, critical business and IT services need to be quickly restored or replaced for timely and effective recovery of the organization. However, fear, uncertainty and doubt can run the show if you don't have well-thought-out and complete recovery plans in place. Even with a plan, the workforce will be operating under a heightened level of stress, such that business-as-usual (BAU) and recovery operating procedures may not be diligently executed. Addressing recovery access requirements, such as recovery team access entitlements, emergency recovery access entitlements, emergency recovery access request workflow and policy violation identification, must be included in IAM and recovery procedures and plans to prevent impeding the recovery process and undoing your IAM infrastructure.

IAM and BCM are key components of IT GRC, and they intersect at four points in each program (see Figure 1).

Figure 1. Where IAM and BCM Intersect

- **IT Service Risk Profiling:** Every IT service must be assessed for its importance to the organization. In doing so, its sensitivity, privacy, criticality and availability time frame are rated as part of its risk profile.

- **Role Life Cycle Management:** Managing recovery access requirements in existing roles, and creating recovery-time-only roles, will better ensure that recovery activities can be executed in a timely manner and can prevent a disaster from occurring due to a lack of access or sabotage (for example, the 2008 San Francisco network administrator fiasco). Others should have the same entitlements in order to maintain the network through a disaster (the administrator may have been hurt and, therefore, unavailable for recovery activities) or to relieve the impact of the sabotage he actually created.
• **Access Policy Violations:** Due to fewer people being available during a disaster, and emergency recovery access being granted, there may be access policy violations—including segregation-of-duty violations—for access to logical and physical assets, including facilities.

• **Recovery Operations:** During a disaster, access needs can change rapidly, and, therefore, provisioning the access to IT services must be done quickly. In addition, additional workforce, such as volunteers, consultants, contractors and people from an adjacent state or work location, may be called in to assist with the recovery effort, and these people need immediate access to IT services. Finally, because of workarounds in business processes at the time of a disaster, ensuring that workers can be authenticated appropriately and in an easy and timely manner may require alternative authentication methods, including out-of-band procedures.

Gartner has defined the following best practices to ensure that your IAM and BCM processes are aligned so that, during a disaster, access to mission-critical business and IT resources is available to the workforce, and the recovery process is not impeded. Integrate each best practice into your IAM and BCM programs to ensure that recovery plans contain the most current recovery access requirements, and the IAM infrastructure is not compromised.

1.0 **Best Practices for Recovery and BAU Access Requirement Alignment**

1.1 **Best Practice No. 1: IT Service Risk Profiling — Classify Your Business Processes and IT Services**

Recovery access requirements for IT service continuity should be defined during the business requirement phase of the business and IT project life cycles. Ignoring this step can result in an IT service not having a disaster recovery strategy and solution that meets the needs of the business, and, therefore, could require significant rearchitecting in order to meet those needs. Gartner recommends a classification scheme (see Figure 2) that groups IT services into recovery service levels that are based on recovery access requirements.
To start, business managers develop a business case for a particular service classification through the business impact analysis process. Service-level definitions should include scheduled uptime, percentage availability in scheduled uptime, and recovery time objectives (RTOs) and recovery point objectives (RPOs). Next, the IT disaster recovery management (IT DRM) team groups like services into classes. Finally, these classes are used to drive the appropriate financial investments and tasks in production and recovery IT service development, architecture, and operations.

As an example, in Figure 2, Class 0 IT services include essential and foundational IT components that need to be recovered before any other IT service is recovered. During an emergency, not all systems are recovered at the same time; however, all authentication systems — from simple user ID and password to strong authentication solutions — must be considered as Class 0 IT services. Class 1 IT services are those that, if unavailable, the enterprise would suffer irreparable harm (they may have been designed and implemented using a real-time enterprise strategy). Not all IT services in a critical business process would be grouped in Class 0, 1 and 2 — rather, only those deemed most critical or with the most downtime effect would be grouped as such. Class 3 and 4 IT services have longer RTOs and RPOs. As recovery times get shorter and shorter, many

<table>
<thead>
<tr>
<th>Class</th>
<th>IT Services</th>
<th>Service Levels</th>
</tr>
</thead>
</table>
| 0     | • Telecommunications  
      | • Networks, VPNs  
      | • Hardware, operating systems, software  
      | • IAM systems   | • 24/7 scheduled  
      | • 99.9% availability (<45 min./mo.)  
      | • RTO = 0 to 4 hours  
      | • RPO = 0 to 15 minutes |
| 1     | • Customer/partner/citizen-facing  
      | • Revenue production  
      | • Supply chain   | • 24/7 scheduled  
      | • 99.9% availability (<45 min./mo.)  
      | • RTO = 0 to 4 hours  
      | • RPO = 0 to 15 minutes |
| 2     | • Less-critical, revenue-producing functions | • 24/6½ scheduled  
      | • 99.5% availability (<3.5 hrs./mo.)  
      | • RTO = 4 to 8 hours  
      | • RPO = 8 hours |
| 3     | • Administrative functions | • 18/7 scheduled  
      | • 99% availability (<5.5 hrs./mo.)  
      | • RTO = 1 to 3 days  
      | • RPO = 1 day |
| 4     | • Departmental functions (not shared with any other group — for example, budgeting) | • 24/6½ scheduled  
      | • 98% availability (<13.5 hrs./mo.)  
      | • RTO = 3 to 5 days  
      | • RPO = 1 day |

VPN = virtual private network  
RTO = recovery time objective  
RPO = recovery point objective  

Source: Gartner (August 2009)
organizations are finding that IT services once classified as Class 3 or 4 become Class 1 or 2 because of the interdependencies between IT services used to deliver the business process.

Once classified, recovery architectures and associated investments are developed for each class, according to their availability service level. At this point, you would start recovery access requirement definition activities using the classes and availability service levels, taking care to not assign excessive access to highly sensitive IT services — even during recovery.

A more-detailed example of IT service risk profiling follows. This manufacturing firm looked at three factors in completing its risk profile: complexity, sensitivity and significance. The resulting scores can then be used as your class definitions in Figure 2. The firm also identified its authoritative sources for user information — a requirement for IAM activities (see Figure 3 and Table 1).

**Figure 3. Application Risk Profiling**

<table>
<thead>
<tr>
<th>Application</th>
<th>Complexity</th>
<th>Sensitivity</th>
<th>Significance</th>
<th>Score</th>
<th>Authoritative Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERP — App.</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>ERP — Oracle</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>ERP — Unix</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Customer Service</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>LiveLink (locations No. 2 and No. 3)</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>LiveLink (location No. 1)</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Active Directory</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>4</td>
<td>✓</td>
</tr>
<tr>
<td>RSA Authentication Manager — RA</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>eProcurement</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>RSA Authentication Manager — 3P</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td>2</td>
<td>✓</td>
</tr>
<tr>
<td>Altiris</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>I/NET 2000</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Source: Electronics Manufacturing Firm, 2007

**Table 1. Manufacturing Firm IT Service Risk Profiling**

<table>
<thead>
<tr>
<th>Score</th>
<th>Complexity</th>
<th>Sensitivity</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Basically impossible to manually reperform system calculations or functionality</td>
<td>Confidential information management status of &quot;Strictly Confidential&quot; or &quot;Confidential&quot;</td>
<td>The system cannot be unavailable for more than 48 continuous hours</td>
</tr>
<tr>
<td>Medium</td>
<td>Manual reperformance of system calculations or functionality is very difficult and would require considerable time and resources</td>
<td>Confidential information status of &quot;Internal Use Only&quot; or other data that should not typically be publicly accessible</td>
<td>The system cannot be unavailable for more than 120 continuous hours</td>
</tr>
<tr>
<td>Score</td>
<td>Complexity</td>
<td>Sensitivity</td>
<td>Significance</td>
</tr>
<tr>
<td>-------</td>
<td>------------------------------------------------</td>
<td>------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Low</td>
<td>Relatively easy or inexpensive to manually reperform system calculations or functionality</td>
<td>Data that may be made publicly accessible</td>
<td>The system cannot be unavailable for more than 240 continuous hours</td>
</tr>
</tbody>
</table>

Source: Electronics Manufacturing Firm, 2007

1.2 Best Practice No. 2: Role Life Cycle Management — Develop Recovery Team Roles and Responsibilities

As part of the BCM planning process, all business units need to be identified and assigned to a particular type of recovery team: the BCM steering committee, the BCM office, the crisis management team, the emergency response team, IT disaster recovery teams, business unit recovery teams and the postmortem team (see Figure 4). Once these teams are defined, the IAM integration process for specific recovery access requirements can be done.
% Figure 4. Recovery Team Identification

<table>
<thead>
<tr>
<th>Who</th>
<th>Team</th>
<th>Steering Committee</th>
<th>Business Continuity</th>
<th>Crisis Management</th>
<th>Emergency Response</th>
<th>IT DRM</th>
<th>Business Recovery</th>
<th>Post-Mortem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior Mgmt.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dept. Manager</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>COO</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td>R</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Risk Management</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td>R</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Facilities</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Human Resources</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Health and Safety</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Legal/Compliance</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Public Relations</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Physical Security</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Customer Mgmt.</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>R (process)</td>
<td></td>
</tr>
<tr>
<td>Fraud Prevention</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Procurement</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Insurance</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>BC Manager</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓ (process)</td>
<td></td>
<td>R (process)</td>
<td></td>
</tr>
<tr>
<td>BC Coordinators</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R (plans)</td>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Info. Technology</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>IT DRM</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>R</td>
<td>✓</td>
</tr>
<tr>
<td>IAM</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Audit</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

R = Responsible
CISO = chief information security officer
BU = business unit
Source: Gartner (August 2009)

It is at this point where you ensure that you have BCM representation on your IAM project team to ensure close cooperation during all IAM and BCM planning activities, as well as recovery execution activities.

1.3 Best Practice No. 3: Role Life Cycle Management — Build Recovery Access Requirements into Existing Roles

Once recovery team types are defined and associated business units are mapped to them, business and IT workforce members can be assigned to the appropriate recovery team and role. Secondary and tertiary workers must also be included, so that, if the primary person is not
available, the secondary or tertiary worker can assume the primary role and fulfill its recovery activities. All recovery team members will be trained to execute the recovery plans associated with their team responsibility when a disaster occurs.

There are three types of activities performed during a disaster (see Figure 5):

- **BAU activities** performed by people not assigned to a recovery team, but who come to a recovery location, or work from home, to perform their regular jobs. They typically don’t need access changes or additional access due to a disaster, but may take on additional responsibilities and, therefore, access, due to a change in the recovery-time workforce in the moment of the disaster event. Also, at the time of a disaster, they would have access to internal disaster services, such as a crisis management website that has been enabled just for the event. Most of the workforce is performing BAU work, even during a disaster.

- **Activities performed by workers** assigned to a business or IT recovery team. They may need additional access to IT services and recovery-specific services in order to perform their recovery team role.

- **High-risk activities** performed by workers who perform privileged or high-risk functions as part of their recovery team responsibilities (business recovery team member, IT recovery team member, crisis management team member, as well as external workers such as the third-party disaster recovery service provider's staff), or are assigned to such activities as a result of the disaster event and are provisioned emergency recovery access entitlements in order to conduct such functions.

**Figure 5. Disaster-Time Activity Types**

Each disaster activity and its associated recovery access entitlements must be provisioned for the recovery effort. Recovery access entitlements can be provisioned in a number of ways:
• Access is provisioned as part of BAU role assignments — for example, the lead Linux administrator or a tertiary backup (neither the primary nor secondary worker is available for recovery efforts). Whenever possible, recovery access entitlements should be built into BAU roles.

• Access is provisioned as part of BAU role assignments, but access is only available during a recovery event. For example, the crisis management internal website used as a communications vehicle to the entire workforce is an IT service used only during a disaster.

• Access is provisioned through explicit recovery roles that are enabled only at the time of a recovery event. Explicit recovery roles should be provisioned with an activation date, as well as a termination date. For example, the use of the role expires 30 days after activation (30 days being the typical planning time frame for which the organization would be in recovery operation mode). The termination date can be manually extended or retracted as the situation dictates. Establishing roles for recovery purposes would be used when there is a need to segregate BAU access from recovery access needs.

Once determined where and how recovery access entitlements should be made available to the workforce, the recovery roles and entitlements should be developed and provisioned for all IT services.

1.4 Best Practice No. 4: Managing Access Policy Violations During a Disaster

The makeup of the workforce may be very different after a disaster than during BAU conditions (see Figure 6). For example, workers might be affected personally by the same disaster as that striking the organization and, therefore, are not available to help the organization recover. No organization should require a worker to be part of its recovery operations.
Managers and other departmental staff may have to take on BAU operations responsibilities that they would otherwise not have to perform. Therefore, during a disaster, these workers may be assigned additional roles or entitlements that can easily create access policy violations between their BAU access and this emergency recovery access, or which would be a violation of least privilege if they were left in place post-recovery. Since there is a high probability that workers assigned emergency recovery access can create access policy violations, all such access requests should be explicitly approved by management prior to the access being granted, and such access should be provisioned with an activation date, as well as a termination date. You should identify as much of this type of emergency recovery access and access policy violations during the IAM and BCM planning processes. However, at the time of disaster, your best-laid plans may not be executable, because each situation is different. You must make decisions based on the specific facts of the situation.

Finally, during a disaster, implementing daily (or more frequent) monitoring of access policy violations is a requirement. The security administration team should be proactive in generating these reports and reviewing them with management.

A summary of recovery activities and recovery access requirements follow (see Figure 7).
1.5 Best Practice No. 5: Recovery Operations — Establish Emergency Recovery Access Request Workflows

Once a disaster is declared, the user-provisioning system can be manually triggered to automatically provision recovery access changes to IT services. These workflows must consider that the request may be initiated by someone not normally assigned to an access request role. For example, the primary manager is not available, and the emergency recovery access request is being made by the tertiary backup (someone not likely to be already defined through the IAM process). The approval process should be as streamlined as possible. For this reason, establishing emergency recovery access request workflows as part of the recovery planning process (as much in advance as possible) is a very important best practice to implement — it avoids adding additional confusion to an already hectic and stressful recovery operations environment. The check-in/check-out workflow used in shared-account or superuser password management tools can help with emergency administrator access.

As part of every recovery exercise, test that these emergency recovery access request workflows and changed access controls work to ensure they are correct.

1.6 Best Practice No. 6: Recovery Operations — Establish Alternative Authentication Methods

Recovery plans may consist of procedures that don't follow BAU processes for a number of reasons — for example, because BAU systems aren't available, or work-around procedures that
take the place of a BAU process are only used during the recovery event. These conditions still require user authentication methods consistent with the criticality and sensitivity of the information to be employed. Authentication management questions that must be answered as part of the recovery access requirements management process include:

1. How do you authenticate users if BAU systems aren't available — for example, bringing foundational IAM systems online at the recovery location?

2. How do you issue authentication credentials when BAU systems aren't available — for example, self-service password change services are not recovered yet?

3. How do you authenticate users to work-around procedures used for recovery purposes only?

The answer to Question 1 is to make authentication systems Class 0 IT services (see Best Practice No. 1 — IT Risk Profiling — Classify Your Business Processes and IT Services). Dual-process logon procedures that rely on root/core-level authentication credentials stored in a vault may be required.

The answers to Questions 2 and 3 might require alternative authentication methods to be deployed during recovery operations. Authentication credentials may need to be issued in advance or on an emergency basis so that work-around procedures can be executed during a recovery — for example, out-of-band authentication using phones can be a low-cost approach with immediate availability for the end users. Ensure that their phone numbers are kept up-to-date just for these disaster situations. Also, there can be potential coverage problems, depending on the location of the end user. In addition, there may be systems (product or developed function) that have to be changed to accommodate a different authentication method. All emergency-use-only authentication credentials should be issued with activation and termination dates.

Consider implementing a versatile authentication server or service to simplify the implementation of multiple authentication methods in multiprocess environments. It can be implemented and integrated only once — making support for alternative authentication methods during recovery much more viable.

1.7 Best Practice No. 7: Recovery Operations — Provision Essential Nonelectronic Resources

Nonelectronic resources (special equipment, facilities access badges for people working at a location different from their BAU location, credit cards, transportation alternatives and so forth) are also needed during a recovery. If you have integrated these assets into the BAU provisioning process, then they must also be considered for recovery purposes. If not, recovery access requirements planning might be your starting point for the provisioning of nonelectronic assets.

Ways to address access to nonelectronic resources needed for recovery purposes include:

- Build nonelectronic resources into role assignments.
- Issue emergency-use-only physical credentials with activation and termination dates.
- Work with government agencies for physical access authorization (for example, Corporate Emergency Access System [CEAS] cards) to facilities involved in the disaster and considered off-limits to all but first responders.
1.8 Best Practice No. 8: Recovery Operations — Disaster Stand-Down: Deprovision Access Changes Made During the Disaster

Finally, after recovery efforts have been completed — the disaster is considered to be in stand-down mode — and the organization is back to BAU operations and facilities, all access provisioned for recovery activities must be deprovisioned in order to avoid a back-door attack through the use of what would be considered excessive access during BAU operations.

Access reports must be generated and reviewed by security administrators to ensure that access provisioned for recovery activities has been deprovisioned and returned to the BAU state for all IAM resources (roles, shared/user IDs, authentication credentials and entitlements), and that violations created during recovery are removed and documented as being removed. This report of post-disaster access should be certified by management.

2.0 Tactical Guidelines

- Put BCM representation on the IAM project team — and IAM representation on the BCM program team — to ensure cooperation is obtained for aligning recovery and BAU access requirements, and that access is properly managed during a disaster.
- Create a risk profile for all business processes and associated IT services.
- Develop a service-level classification system with associated production and recovery development, infrastructure, and operations architecture requirements.
- Include IAM systems as Class 0 IT services.
- In as advance of a disaster as possible, document potential access policy violations due to emergency recovery access.
- Have emergency recovery access request workflows ready for use.
- Test emergency recovery access request workflows and changed access controls during recovery exercises.
- Issue emergency entitlements, authentication credentials and physical access credentials with activation and termination dates.
- Use out-of-band authentication. Work with government agencies for physical access (for example, CEAS cards) to off-limits facilities.
- Actively monitor privileged and emergency recovery access usage for access policy violations during the disaster.
- Build nonelectronic resources into role assignments.
- Deprovision emergency entitlements after the disaster stand-down.
- Perform an access certification after the disaster stand-down. Obtain senior management attestation of the post-disaster access certification.

RECOMMENDED READING

"Research Roundup: Business Continuity Management and IT Disaster Recovery, January 2009"
"Business Continuity Management Defined, 2008"
"Hype Cycle for Business Continuity Management, 2009"
"A Simple IT Risk Management Process"
"Workforce Continuity Defined"
"Enlightening the CEO on Business Continuity Management"
"Best Practices for Conducting a Business Impact Analysis"
"MarketScope for Segregation of Duty Controls Within ERP and Financial Applications"
"Manage Segregation of Duties in ERP and Financial Systems to Address Audit Findings and Business Process Conflicts of Interest"
"MarketScope for Shared-Account/Software-Account Password Management"
"Superuser Privilege Management Tools for IBM i, Unix and MS Windows Server Operating Systems"
"MarketScope for Enterprise Broad-Portfolio Authentication Vendors"
"Versatile Authentication Servers and Services"
REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glany
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509