FORRESTER®

For: Infrastructure & Operations Professionals

Execute The Five Key Processes Of The Business Technology Resiliency Life Cycle

by Stephanie Balaouras, February 24, 2014

KEY TAKEAWAYS

To Improve BT Resiliency, I&O Pros Need To Prioritize Process Excellence

Technology such as clustering and replication can improve the availability of specific systems, but they don't address broader issues that negatively affect recovery capabilities, such as increasing technology complexity and the continued lack of thorough testing. To really see a marked improvement in resiliency, you must strive for process excellence.

I&O Pros Must Master Five Essential BT Resiliency Processes

All the standards for business continuity or IT disaster recovery, with some minor variation, follow this process life cycle: 1) business impact analysis; 2) risk assessment; 3) strategy development and response plan documentation; and 4) exercising, testing, and maintenance. Forrester adds a fifth process: integration with availability management.

Resiliency Is Not A One-Time Planning Event; It Is A Continuous Life Cycle

Resiliency is not a one-time planning effort; it is a continuous life cycle. Thus, you must embed each of the five processes in BT operations; maintain a current understanding of business context and risk; adjust strategy whenever the business or technology environment changes; update plans continuously; and exercise and test frequently.

Execute The Five Key Processes Of The Business Technology Resiliency Life Cycle

Processes: The Business Technology Resiliency Playbook

by Stephanie Balaouras and Eveline Oehrlich
with Rachel A. Dines and Heather Belanger

WHY READ THIS REPORT

This report outlines Forrester's solution for infrastructure and operations (I&O) leaders responsible for developing and implementing the core processes that support business technology (BT) resiliency. The core processes include business impact analysis (BIA); risk assessment; strategy development and response plan documentation; and exercising, testing, and maintenance. In addition, any resiliency efforts must also integrate and support ongoing efforts to improve overall availability management with the environment. Thus, Forrester adds a fifth process to the life cycle: integration with availability management. Once you define your standard processes, I&O leaders must also define policies that dictate the frequency of updates and refreshes as well as the use of specific templates, tools, and document repositories. Without repeatable processes and clear policies, guidelines, and standards, BT resiliency becomes nothing more than a one-time planning exercise where plans sit on shelves gathering dust. This report describes each of the core processes of the BT resiliency life cycle and provides key recommendations for successful implementation.

Table Of Contents

Notes & Resources

In developing this report, Forrester drew from a wealth of analyst experience, insight, and research through advisory and inquiry discussions with end users, vendors, and industry experts.

Related Research Documents

Elevate Your Business Technology Resiliency Program With An In-Depth Strategic Plan
April 8, 2013

Assess The Maturity Of Your Business Technology Resiliency Program
October 15, 2012

Develop Your Business Technology Resiliency Balanced Scorecard
April 30, 2012

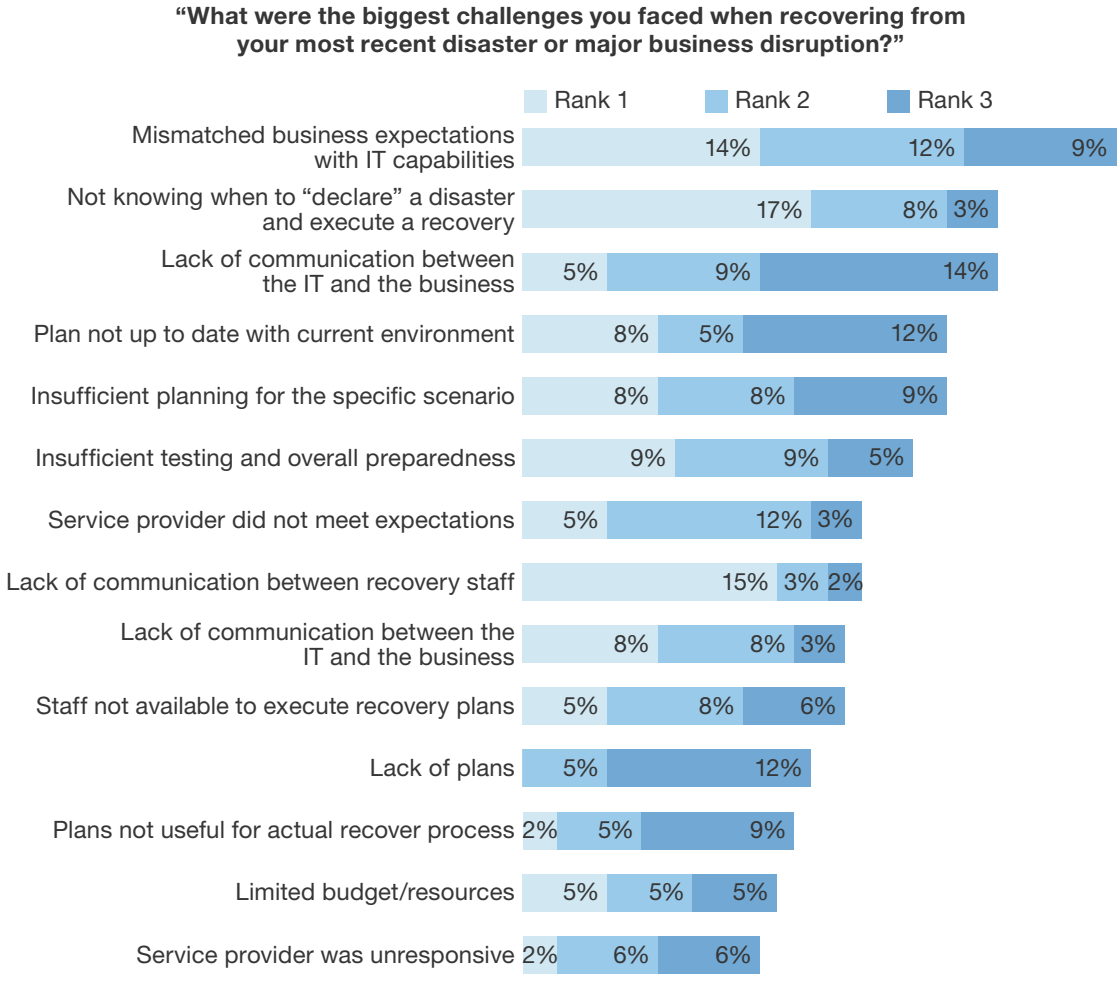
TO IMPROVE BT RESILIENCY, PRIORITIZE PROCESS EXCELLENCE

Our most recent joint survey with the Disaster Recovery Journal (DRJ) uncovered two disturbing trends. First, business continuity and disaster recovery (BC/DR) decision-makers indicated that their recovery capabilities — recovery time and recovery point — had actually increased in length despite stronger adoption for advanced recovery technology such as replication. Second, when we asked decision-makers who had experienced a disaster to identify their top challenges, the top five challenges indicated that a lack of process maturity is to blame for most of the issues (see Figure 1). We believe that improving process maturity will not only improve the execution and success of actual disaster declarations, but that it will also improve recovery objectives. Technology such as virtualized high availability, replication, and continuity automation can improve the availability and recovery of specific systems, but they don't address broader issues that are negatively affecting recovery capabilities, such as increasing IT complexity and the growing number of critical systems. For successful recoveries, you must be able to:

- **Orchestrate the recovery of IT services that have intricate dependencies.** For a large enterprise, business processes are now a composite of IT services delivered on-premises or via a cloud or managed service provider. These IT services are in turn a composite of hundreds of apps, middleware, databases, and infrastructure assets (e.g., server, storage, and network). Business owners view recovery and downtime from a customer perspective, making sure that they have what they need to win, serve, and retain customers. Unless business processes are fully functional, it doesn't matter whether individual systems are available. As a BT resiliency pro, it's therefore your job to ensure that you can orchestrate the recovery of all IT services and assets in the proper sequence to ensure that business processes are available end to end. You will need to understand which processes rely on which specific IT services and assets and when the business expects them back; you need to have a continuously updated business impact analysis (BIA).

- **Execute your plans confidently when it's time to do so.** When Hurricane Sandy struck the Northeast US in October 2012, we discovered that the majority of companies in the affected region failed to activate their DR plans in anticipation of a direct hit, despite ample warning.[1] Why? Several technology managers told us they didn't have any confidence in their DR plans, and so they waited until the last possible second to activate their plans in the hope that they could ride out the storm. This strategy backfired for several of them. Once the storm hit, it knocked out power for days, exceeding the amount of diesel fuel that companies had on hand to run backup power generators. If you're not testing and updating your plans regularly and adjusting your strategy and plan scenarios based on new information, then you might as well not have any plans.

Figure 1 Recent Declarations Reveal Significant Process Challenges



Base: 66 global disaster recovery decision-makers and influencers who have declared a disaster or had a major business disruption (multiple responses accepted)

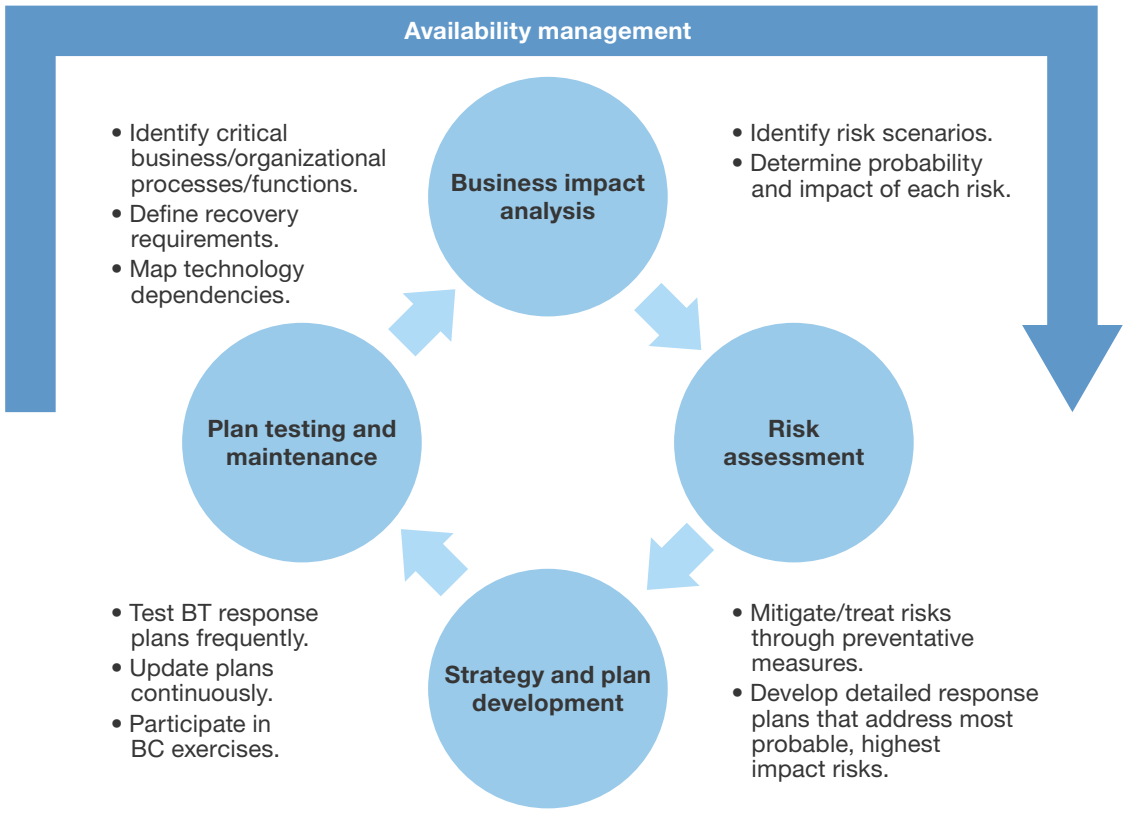
Source: Forrester/Disaster Recovery Journal Crisis Communication, Risk Management, And Business Continuity Survey, Q4 2013

61521 Source: Forrester Research, Inc.

I&O Pros Must Master Five Essential BT Resiliency Processes

During the last five to six years, we have seen a coalescing of recognized business continuity and disaster recovery processes and best practices around standards such as the National Fire Protection Association 1600, ISO 22301 (based predominantly on British Standard 25999), and ASIS SPC.1-2009. Whichever standard you select, they all, with some minor variation, follow this life cycle: 1) BIA; 2) risk assessment; 3) strategy development and response plan documentation; and 4) exercising, testing, and maintenance. And Forrester adds a fifth process: integration with availability management (see Figure 2). If you want to improve your capabilities and increase your confidence in your preparedness, you must adopt a standardized process framework (it can be one of your own, one of ours, or one of the recognized industry standards) and make its implementation and continued improvement your top priority (see Figure 3).[2]

Figure 2 The BTR Life Cycle



61521 Source: Forrester Research, Inc.

Figure 3 Bringing All The Phases Together — A Summary

	Who	What	When	How
Business impact analysis	Generally run by the business continuity group with strong support and input from the BT resiliency team.	The BIA is the process that determines the relative criticality of all business services and maps all of their resource dependencies. It also quantifies cost of downtime and determines appropriate recovery objectives.	The technical dependency mapping from the BIA should be updated continuously. Identification of critical business process and other resource dependencies should be reviewed whenever there is a change in the business or at least annually.	BIAs are generally conducted via surveys, in-person interviews, and workshops. BC and GRC tools can help field surveys and consolidate data and integrate data automatically from systems of record.
Risk assessment	A BC or enterprise risk management group would drive risk assessments focused on operational risks. BT resiliency team should run risk assessments focused on technology risk.	The purpose of the risk assessment is to identify, analyze, evaluate, and treat risks. BC and BT resiliency pros should focus treatment efforts and response plans on the most probable, highest impact risks.	Risk assessments should be updated at least annually or whenever new information or changes in the business or IT environment necessitate a review of risk assumptions.	Risk assessments are conducted via surveys, in-person interviews, workshops, secondary research, and risk/threat intelligence services. BC and GRC tools can help track, analyze, and evaluate risks.
Strategy and plan development	BC teams will develop business prevention strategies and develop overarching BC plans. The BT resiliency team is responsible for the technology equivalents. BT response plans must ultimately roll up to a BC plan.	Strategy should focus significantly on preventing disruptions through risk treatment. For risks that can't be treated or for any unacceptable residual risk, there should be specific BC and BT response plans that coordinate the organization's response to the disruption.	Strategy should be adjusted after any update or refresh of the BIA. New plans should be developed or existing plans updated as a result.	Prevention strategies for business disruption must be embedded in business and operational strategy. Likewise, prevention strategies for IT disruption must be embedded in technology architecture. There is a wide variety of sample plans, including many in BC and GRC tools. Plans should be consistent and maintained in a central repository that is also accessible remotely via a mobile device or web browser.

61521 Source: Forrester Research, Inc.

Figure 3 Bringing All The Phases Together — A Summary (Cont.)

	Who	What	When	How
Plan testing and maintenance	BC and BT resiliency teams lead their own exercises (BC) and tests (BT), but both teams should be heavily involved. Each team is also responsible for ensuring their plans are up to date, complete, and thorough.	Exercises and tests help to validate preparedness and stated recovery capabilities. They also help to identify any issues or gaps in strategies or specific response plans. Finally, they are also an effective means of training employees in their roles and responsibilities. Not only must plans be thoroughly exercised and tested, they should be kept up to date to reflect changes in business or BT operations. If plans are out of date, they will hamper recovery efforts during exercises/tests and real disruptions.	Both BC and BT resiliency teams should run multiple types of exercises/tests frequently each year, including plan walkthroughs, tabletop exercises, component exercises/tests, and full exercises/tests. BC plans should be updated anytime there is a change to the BIA or a BC exercise reveals a weakness in the plan. BT plans should be updated continuously as part of change and configuration management or whenever a test reveals a weakness in a plan.	Exercise and test policies should be documented and enforced by central governance teams. As exercises/tests are conducted, BC or GRC tools can help track and report on results. Plans are best stored in a central repository ideally with a BC or GRC tool that can cascade any change to a business or BT context to all affected plans in the repository.
Availability management	At larger or more mature organizations, availability management is run by an availability manager in conjunction with service owners and IT operations managers.	Availability management is the process to define, analyze, plan, measure, and improve all aspects of the availability of IT services.	Availability management is a continuous process that constantly monitors the uptime of critical components and services, as well as conducts failure analysis and ensures SLAs are met.	Service management and automation tools are the core foundation of tracking and analyzing data for availability management. Availability monitoring and management tools are also key for gathering information on service availability.

61521 Source: Forrester Research, Inc.

THE BIA IDENTIFIES BUSINESS PROCESSES AND MAPS RESOURCE DEPENDENCIES

The BIA is an essential, but often overlooked, step in the BT resiliency life cycle. It helps BC and BT resiliency teams identify your organization's most critical business processes and the dependent resources (e.g., people, physical facilities, and technology services) required to maintain the availability of those processes. It also helps you: 1) determine appropriate recovery objectives (e.g., recovery time and recovery point) for each process, and 2) quantify the impact that a major disruption would have on revenue, productivity, and customer experience. To ensure that BIAs are current and relevant, we recommend that you:

- **Employ multiple techniques to gather the data necessary for a complete BIA.** To gather all the data necessary for the BIA, you'll need to field web-based surveys to a broad swath of employees (e.g., tenured individual contributors, managers, and directors), conduct in-person interviews with business owners (i.e., every leader responsible for a profit and loss statement and the heads of all corporate functions, such as marketing, finance, and customer service) and then host workshops with both of these audiences to further work through and analyze all the data you have gathered (see Figure 4). The goal is not only to arrive at detailed process mapping but to achieve agreement on *realistic* availability service-level agreements or specific recovery objectives (recovery time and point).

  Expert tip: Business continuity management (BCM) and governance, risk, and compliance (GRC) software tools can help you design, field, and analyze BIA surveys so that business process owners and other stakeholders can help you identify critical processes, resource dependencies, and recovery objectives. You can also manually enter or upload data gathered via in-person interviews and workshops. The ultimate benefit is that you have all your data in a relational database that you can analyze more effectively than you could in spreadsheets and documents.[3]

- **Use process-modeling to visualize critical interrelationships and dependencies.** BCM and GRC tools can serve as repositories to visually define and track business processes and dependent resources. In addition to the data you collect via BIA surveys, interviews, and workshops, some of these offerings can import resource data from HR, Active Directory (AD), configuration management databases (CMDBs), and other systems via application programming interface (API) or simple file upload. Even more advanced offerings also offer the ability to automatically discover and graphically model business processes and their dependencies. The visualization can help you identify hereto unknown dependencies and perform "what if" scenarios (e.g., what the impact is if a particular IT service is unavailable).

  Expert tip: Particularly for technology resource dependencies, it's ideal to enable automatic updates from systems of record like HR, AD, and CMDBs rather than rely on gathering this data manually. In fact, for complex environments that have thousands of technology resources and a high rate of change, this is essential. Otherwise, your BIA mapping is either incomplete, out of date, or both.

- **Strive for a continuous BIA process.** This recommendation is aspirational. Today, most BC and BT resiliency professionals conduct full BIA refreshes every two to three years and conduct updates annually.[4] However, in today's dynamic business environment where firms are constantly entering into new business partnerships, expanding their geographic presence, and acquiring businesses and spinning off others, you don't want to wait two years to update your BIA. If you have a complex organization, don't try to run a BIA across your entire organization. BIAs should be specific to a local geography or to a business unit.

Expert tip: Business owners often complain that they must complete multiple surveys from different teams, including operational risk management teams, BC/DR teams, and security teams — all of whom ask very similar questions.[5] For the most part, all of these teams are seeking to gather contextual information about the business and its dependencies for planning purposes. As much as possible, rather than run your own separate BIA, try to run one in conjunction with these other teams. Often you'll find that a BC or other risk management team has already invested in a BC or GRC management tool that you can use as well; avoid purchasing yet another tool for ongoing program management.

Figure 4 Key Questions To Ask During The Business Impact Analysis

To determine the appropriate recovery time and recovery-point objective during a BIA, you should collect the following types of information from business owners:

What are my company's most essential business processes?	Examples might be order-to-cash, supply chain management, and financial accounting and reporting.
What are the dependent IT systems for each business process?	This dependency mapping is one of the most difficult steps to accomplish because basic business processes often rely on multiple integrated IT systems, and the sequence of recovery is critical in a recovery scenario. There are some technologies, such as a configuration management database, that can assist with this dependency mapping and even automate the mapping.
How quickly do I need to restore these critical processes?	What is the business' sensitivity to downtime of the dependent IT systems? Do I have any manual workarounds?
How much data can I afford to lose for each of these critical processes?	Is there some data that can be recreated if necessary? How often should the data be backed up locally, and how often should the data be transmitted off-site?
What would be the cost of downtime and data loss?	What would be the impact on company revenues, profitability, customer service, worker productivity, and compliance if the business process was unavailable and some data was lost?

Expert tip: Instead of asking business owners how much downtime and data loss they can endure from their critical applications (spoiler alert: the answer will usually be zero), use these questions to understand the customer, revenue, employee, and partner impacts that will lead you to developing a realistic and appropriate RTO and RPO.

61521 Source: Forrester Research, Inc.

The Risk Assessment Identifies, Analyzes, Evaluates, And Treats Risks

After the BIA, or as a part of the BIA, you must conduct a local risk assessment to understand the likeliest and most impactful risks (e.g., extreme weather, natural disasters, human-made disasters, pandemics, IT failures, or other disruptions) that you need to mitigate. You can identify threats via surveys to business owners closest to their operations, via workshops with cross-functional teams, via your own secondary research, and also via risk/threat intelligence services. As part of this process, you'll want to analyze and evaluate the risks in order to *quantify* the likelihood of their occurrence and their impact to the business (see Figure 5). You'll then want to track them in a risk register. Focus your treatment or mitigation efforts on the most probable, highest impact risks. If your organization opts not to address a particular risk, then a business executive (typically a C-level exec) must sign off on the acceptance of the risk. To ensure that risk assessments are current and accurate, we recommend that you:

- **Build a formal risk taxonomy to serve as a classification system.** How do you go about identifying and classifying risks? There are many industry risk taxonomies to use as potential starting points, including the COSO ERM framework (broad categories of risk), Basel II (operational risks), Software Engineering Institute (software development risks), NIST Special Publication 800-30 (information security and other technology risks), and PMI (project risks).[6]

  Expert tip: For BT resiliency planners, NIST Special Publication 800-30 is perhaps the best choice. It offers three categories of threat sources related to information security and technology risks. These categories are natural threats (e.g., floods, earthquakes, tornadoes, landslides, avalanches, and electrical sources); human threats (e.g., unintentional acts such as inadvertent data entry or deliberate acts such as cyberattacks); and environmental threats (e.g., long-term power failure, pollution, chemicals, and liquid leakage). This is not only helpful for US federal government agencies that must follow NIST guidelines but any organization that conducts or plans to conduct any business with the US federal government or organizations that are part of the defense industrial base. For those outside the US, it's still a good starting point.

- **Employ multiple techniques (and sources) to get a well-rounded perspective.** Similar to the BIA, you'll need to employ multiple techniques (such as surveys, brainstorms, and workshops) to complete the risk assessment. You'll also need to gather your own secondary research from government sources and risk/threat intelligence services. In the US, Federal Emergency Management Agency (FEMA) provides maps and a list of declared disasters by state. The United Nations also provides a list of government and quasi-government agencies that track and manage natural disasters.[7]

  Expert tip: Once your BCM or GRC software tool is populated, it will also help you conduct what-if scenarios to determine possible outcomes of certain risk events. Some software offerings will provide actual statistics for historical threats for certain geographies and some will allow you to overlay flood, severe weather, and volcano maps.

- **Constantly challenge your risk assessments.** Similar to BIAs, our research shows that many BC and BT resiliency pros update their risk assessments every two to three years. And in some cases, individuals never challenge their own long-held assumptions about risks. Out-of-date assessments or maintaining outdated perspectives of risks can be disastrous. Imagine if the risk managers of the Fukushima nuclear power plant had questioned some of its original design specifications after they witnessed the 9.3 earthquake and resulting 30-meter (98-foot) tsunami that hit the Indian Ocean in 2004. The Fukushima nuclear plant, first commissioned in 1971, was designed to withstand only an 8.7 earthquake and a 5.7-meter (19-foot) tsunami. Once they realized that a 9.3 earthquake was very possible, they might have recommended building up the sea walls at the plant or ensuring that backup power generators weren't located on the ground — both of which might have avoided the nuclear crisis in 2011.[8]

  Expert tip: Ideally, you're taking a fresh look at your risk assessments annually, but in between, you want to make it a practice to constantly revisit the sites where you gather intelligence about extreme weather/natural disasters, transportation accidents, hazardous material spills, and energy accidents (e.g., incidents at nuclear power plants and natural gas facilities). You can also subscribe to a number of risk intelligence feeds and weekly trends reports from a variety of vendors. You'll find feeds and trends reports that specialize in cybersecurity (e.g., Cyveillance), regulatory changes (e.g., IHS, LexisNexis, SAI Global), and other risk domains. The goal is to keep yourself informed on changing risk trends. You'll also want to urge coworkers and other colleagues during your interviews and workshops to feel comfortable challenging your assumptions.

Figure 5 Sample Risk Assessment Criteria

Suggested criteria	Explanation
Category	The type of risk according to your taxonomy
Risk	A word or phrase that names the risk event or situation
Description	An explanation of the risk event or situation
Cause(s)	The event, threat, attacker, or other trigger that brings the risk to fruition
Target(s)	The location, asset, process, or objective affected by the risk
Consequence(s)	A description of what the effect would be on the target
Existing control(s)	An explanation of any current efforts, processes, technologies, or other factors (if any) that might modify the risk's likelihood or impact
Likelihood	An estimate of the potential that a risk will occur in a given time frame. This may include measures of inherent (without existing controls) and residual (with existing controls) likelihood.
Impact level	An estimate of the severity of the effect on the target. This may include measures of inherent (without existing controls) and residual (with existing controls) impact.
Effort to remediate	An initial estimate of how much effort would be needed to mitigate the risk to an acceptable level
Owner	The name of the individual accountable for the management of the risk
Action	A recommended or agreed-upon response to the risk
Urgency	A rating of how critical a timely response to this risk is
Date	The deadline for any necessary action and/or reassessment
Status	The current condition of the risk and/or any relevant actions

61521 Source: Forrester Research, Inc.

The Strategy And Plan Development Formalizes Your BTR Practice

Part of the strategy development overlaps with the risk assessment process. One of the most important components of strategy is to implement preventative measures to mitigate risks. You'll want to treat or mitigate the most probable, highest impact risks, and, for any unacceptable level of residual risk, ensure that you have a detailed response plan in place. For example, if a history of IT hardware, software, and human error has led to significant downtime for a critical system (e.g., email, ERP, or CRM), part of your risk treatment plan includes the hardening of the system through a high-availability cluster or even outsourcing it to a cloud or managed provider who can offer a much better availability SLA than you can achieve yourself. However, both treatment plans still have residual risk. In the former, you could still suffer a data-center-wide event, and in the latter, there is no 100% guarantee that that provider will not suffer its own outage. Thus, you'll still need response plans that will address how your organization will respond if these *specific* scenarios occur. To ensure that strategy and plans are viable, we recommend that you:

- **Design resiliency into your BT architecture.** The best resiliency strategy is to avoid any downtime. This means that you design resiliency into both your technical architecture and your business operations and processes, not try to bolt it on afterwards (see Figure 6). From a technology perspective, it starts with a minimum of N+1 redundancy in all physical data center components as well all IT infrastructure. It then extends to the development and delivery of your applications and supporting middleware, databases, and operating systems. Developers must build apps for resiliency (e.g., to run in a cluster or an active-active configuration) and security. And as more apps, platforms, and infrastructure move to the cloud, you'll want to work with your sourcing and vendor management (SVM) team to ensure that cloud providers have their own mature BC/DR and backup processes and technologies in place — don't take anything for granted.

  Expert tip: A significant number of disaster declarations are attributable to rather mundane events such as power outages and IT failures (hardware, software, and human) — two risks that you should be able to easily mitigate with backup power generators (with a reliable source of diesel fuel) and IT redundancy. However, as IT complexity and increasing business reliance on technology exacerbates availability and recovery challenges, you'll want to work with enterprise architecture (EA) teams and your CIO to address complexity. First, you'll want to advocate for the rationalization of applications (some large enterprises can have thousands of apps, new and legacy). Second, you'll want to advocate for the consolidation, simplification, and standardization of IT infrastructure. You'll also want to limit the number of recovery approaches to no more than three to four (one for each tier of service that you offer, such as mission-critical, business-critical, and business-supporting). Not only will this make it easier to orchestrate recoveries, but it will make it feasible to automate recoveries with tools such as VMware's Site Recovery Manager, PHD Virtual Reliable DR (VirtualSharp), or Neverfail.

- **Use analytics to predict failure.** Proactively identifying the failure of IT services and technology components should be supported by leveraging a variety of analytical management capabilities. The prerequisite to proactive predictions of failure is that the IT service has an agreed upon service level, is instrumented with management solutions that support the prediction of one or more issues, and that there are processes — such as incident and problem management — associated with addressing the issues before they can cause problems to the business and service consumers. The IT service needs to be understood and managed with all its dependencies and relationships (as stated above). Tools to predict broader failures are emerging as well, such as solutions that correlate data from internal and external sources like weather feeds, local government alerts, and transit information, and they can make recommendations relative to the likelihood of failure. IBM's SmartCloud Intelligent Operations Center is a good example of this.

  Expert tip: The landscape of IT analytics tools is wide and broad. They all have the ability to churn through large volumes of data and recognize patterns to proactively identify issues. These patterns are then used to issue alerts and events to the responsible team. However, these tools can't predict all downtime and potential downtime, because every organization faces a different set of challenges, resulting in different patterns. Some of your existing tools might already have such capabilities. Be pragmatic; define the initial tool requirements and identify what is already deployed that can be used and shared to get started as quickly as possible. Where basic tools are not already available, work with other technology management teams — such as the application development, architecture, and operations teams — to identify common requirements when looking at new solutions.

- **Develop and document *scenario*-specific plans.** One common mistake that BT resiliency pros frequently make is to develop just one or two response plans — usually to address when the data center is a "smoking hole." However, in reality, the likelihood of a smoking hole is relatively low. A response plan for a power failure is significantly different than a response plan for a distributed denial of service (DDoS) attack of your eCommerce site. Having scenario-specific response plans shows that you know you can't respond to an event with a boilerplate plan; different scenarios — pandemic, IT outage, power failure, telecom failure, cyberattack, extreme weather — require customized responses. It can be useful to think about technology risks as falling into the following four categories: 1) short-term disruption with no lasting damage (e.g., short network outage); 2) long-term disruption with no lasting damage (e.g., long power outage); 3) long-term disruption with lasting damage (e.g., flood); and 4) disruption in physical access and staffing only (e.g., transportation disruption or pandemic).

  Expert tip: Clients frequently ask for BC and BT response plans. For a BT response plan, we always recommend that I&O pros use the template within NIST Special Publication 800-34 as a starting point.[9] The guide and the template within are very thorough. You can tailor the template to suit your organization. If you do modify it, it's important that you don't forget certain steps, such as activation/declaration criteria, failback, and salvage tasks (see Figure 7). When activation

criteria are not clear, BT resiliency managers often waste precious time deciding whether they should activate the plan. Once you have successfully activated your plan, at some point, after the crisis has subsided, you'll need a plan for how you will fail back — and make no mistake, failing back to your production site is just as difficult as failing over to your recovery site. BC or GRC tools will also have sample templates.

Figure 6 Sample Risk Mitigation And Prevention Strategies

Technology	Business
• Select data center locations with a low threat profile. • Ensure physical access security and reinforce building integrity. • Provide regularly tested backup generators and UPS systems. • Create local and geographic redundancy in IT architecture (e.g., clustering, active/active data centers). • Select IT infrastructure with N+1 component redundancy. • Provide telecom network redundancy. • Provide multiple diverse connections to the power grid. • Ensure that good change and configuration management practices are in place. • Reduce IT complexity through standardization. • Develop software applications for resiliency and security. • Cross-train IT employees; provide remote management and administration capabilities. • Proactively monitor for threats.	• Select work and office locations with a low threat profile. • Ensure physical access security at all locations. • Provide regularly tested backup generators and UPS systems at all locations. • Cross-train employees in multiple job functions. • Develop the ability to shift workloads to other work locations in the event of disruptions. • Have redundant supply chain and manufacturing relationships. • Enable remote access/work-from-anywhere technical capabilities for the majority of employees. • Have additional employee sourcing options at your disposal. • Document and train employees in all manual workarounds. • Ensure that there is extensive communication via multiple modes. • Have clear executive and management succession. • Proactively monitor for threats.

61521 Source: Forrester Research, Inc.

Figure 7 Essential Response Plan Components

Plan components	Explanation
Scope	What is the scope of this specific response plan? Business continuity? IT resiliency?
Background information	Necessary background information about location of facilities, recovery sites, and partner sites, IT architecture, etc.
Response team	Names and contact info for core response team, external parties (e.g., first responders, vendor and service partners)
Activation criteria	How much downtime is allowed before the plan is triggered?
Communication/ notification	Customized notification and ongoing communication with management, employees, patients, partners, external groups, etc.
Response/recovery tasks	Specific sequence of tasks to recover operations
Salvage tasks	Tasks to salvage equipment and resources from primary facilities
Failback tasks	How the organization will resume normal operations after the disruption has ended
Test	Strategy and schedule of plan tests, as well as results

61521 Source: Forrester Research, Inc.

Planned Testing And Maintenance Validates Preparedness And Helps Close Gaps

If you're not exercising and testing your plans, your plans are useless. While this may seem harsh, it is true nevertheless. Conducting exercises and tests has several benefits: 1) validates your stated recovery capabilities; 2) uncovers errors or issues in your plans (better to find out now than during an activation); 3) trains business and BT employees in their roles and responsibilities; and 4) continuously challenges assumptions in your plan. In short, frequent exercising and testing leads to confidence and success. If you're confident in your plans, you'll avoid hesitation and activate them when appropriate; you'll also execute your plans more smoothly because you, your response team, and your business users know what they are doing.[10] To ensure that testing is thorough, we recommend that you:

- **Test to find issues.** Testing is difficult; it takes up staff time, and, depending on the test, it may even lead to some production downtime. As a result, too many I&O pros approach resiliency tests as a checkbox item. They don't test frequently enough and when they do, the goal is to get through the test in the least amount of time possible to satisfy technology management leaders and auditors. One of the main benefits of testing is finding problems in a controlled environment rather than during a disaster declaration. If your testing has been problem-free, you probably aren't looking hard enough or you aren't testing thoroughly enough.

Expert tip: Take advantage of multiple exercise and test types. Walk-throughs and tabletop exercises are great opportunities for both business and technology management employees to familiarize themselves with plans, uncover issues, and question assumptions (see Figure 8). For component and full tests that require an actual or simulated failover, consider expanding the objectives of the test to include not only achieving stated recovery objectives but training. Also, be careful how you incentivize employees; it often has unintended consequences. You want employees to point out potential issues, not sweep them under the rug to expedite the test. Finally, to help reduce the time and complexity of testing, continue to advocate for consolidation and standardization and the adoption of virtualization and management tools that can help automate failover and failback.

- **Include both the BC team and business partners in tests.** Every exercise and test (and subsequent debrief) should include members of the BC team since, ultimately, your response plan rolls up to an overarching BC plan and the plans need to integrate seamlessly. In addition, your plan needs to include critical "human" elements, such as communication, which BC planners can help you get right.[11] In addition to the BC team, for certain tests, you'll also want to include dependent business partners such as outsourcers, managed service providers, cloud providers, and contractors. In today's extended enterprise, rarely, if ever, is a business process self-contained within an organization's four walls; it is almost always a composite of internal and external services. Thus, if your dependent partner is down, your organization is down.

  Expert tip: According to a joint Forrester/Disaster Recovery Journal survey on BC readiness, 51% of BC influencers and decision-makers report that they do not assess the readiness of their partners.[12] Even among those organizations that do assess partner BC readiness, their efforts are superficial. Only 17% include partners in their own tests, and only 10% conduct tests specifically on their critical partners.[13] This is one of the biggest risks in resiliency today. To address it, before it becomes a nightmare, you'll need to work closely with your SVM team during the vendor selection process to negotiate for the frequency and extent of partner participation in your resiliency exercises and tests. Requesting or insisting on participation after contract and SLA negotiation is not likely to be fruitful.

Figure 8 Exercise/Testing Types And Frequencies

	Description	Frequency
Walk-through exercise	Reviewing the layout and contents of a plan	As necessary to familiarize response teams and individuals with a documented plan or changes to a plan
Tabletop exercise	Using a scenario, discussing the response and recovery activities of a documented plan	At least three to four times per year
Component exercise	Physically exercising a component of a documented plan (e.g., testing automated communications services or work-from-home capabilities together with IT or building evacuation procedures or partner capabilities)	As necessary as major changes are made to the business or IT operating environment. Once to twice per year until you have cycled through all components not included in a full exercise.
Full exercise/ simulation	Using a scenario, carrying out the response and recovery activities of a documented plan or for an entire organization	At least once per year; twice is ideal. This is most often done as a simulation rather than an actual failover of business operations.

61521 Source: Forrester Research, Inc.

Your BT Resiliency Processes Must Underpin Availability Management

Availability management is critical in today's always-on, always-available world, as the availability of IT services has a direct impact on the reputation of the business. This process must be considered in all states of the service life cycle, from its strategy, design, transition, and operation to its continual improvement. The process itself does not directly address BT resiliency as a topic but has a close relationship with the assessment and management of the risks associated with the IT services at stake. Thus, we recommend that you:

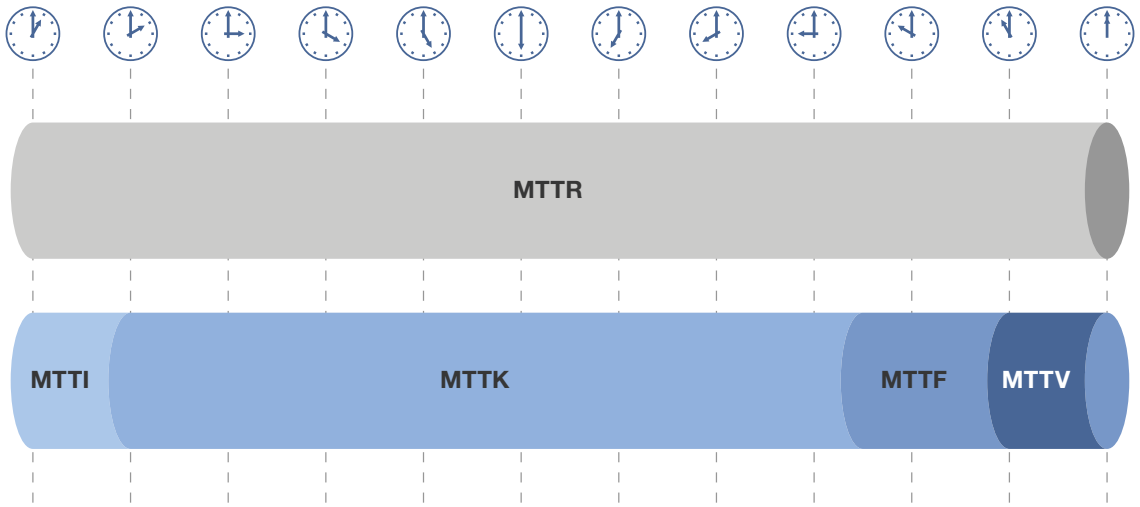
- **Consider both the end-to-end service and individual component perspective.** From the perspective of the business user, a service is only available if it serves its function in supporting the business capability or process. Traditionally, technology management organizations focused their efforts on individual component availability, and this often created a disconnect between technology management and the business. While much depends on the nature of the business operation, it's always important to manage and understand both the availability of a business/IT service and availability of the architectural components. An excellent example of this concept is the customer-facing service of an ATM machine. From technology management's perspective, an ATM may appear available because all components are running as expected, but if the ATM can't be physically accessed due to environmental issues such as flooding, the customer will consider it to be not available.

Expert tip: When designing, managing, and reporting availability, you need to embrace both the individual components that are supporting the service and the availability of the entire service. The CIO's organization needs to have a new and refined awareness of user experience and how technology is used to support the business. This is ensured by leveraging and inserting service owners into the definition of availability and resiliency discussions. Service owners have a good understanding of the makeup of a business or IT service and can add an incredible amount of knowledge to cover the end-to-end dependencies of such.

- **Remember that not all is lost when things go wrong.** The incident management process is typically used to restore business and IT services as quickly as possible. The typical metric to measure incident restoration is mean-time-to-restore (MTTR). Each incident goes through four major stages: 1) mean-time-to-identify (MTTI); 2) mean-time-to-know (MTTK); 3) mean-time-to-fix (MTTF); and 4) mean-time-to-verify (MTTV). To be much more effective in restoring services and technology components, you should break down your incidents into these four life-cycle stages for much better details on how to improve each life-cycle stage separately (see Figure 9). For example, system management solutions that use automated alerts and automated recovery can reduce MTTF significantly. Other examples are descriptions of escalation procedures, which allow the reduction in MTTK and, therefore, speedier focus on MTTF.

  Expert tip: Use the incident life-cycle approach to work with your incident management and problem management process owners to see how the availability of a service or component can be broken down into subcomponents. This should be a joint effort between the BT resiliency and operations team, as both teams have the same goals to restore and eliminate total downtime perceived by your business partner or users. Using this approach will allow you to identify inefficiencies and ultimately will reduce the business impact.

Figure 9 Deconstruct MTTR To Find Improvement Opportunities



61521 Source: Forrester Research, Inc.

WHAT IT MEANS

CONTINUOUS IMPROVEMENT IS THE SIXTH PROCESS

For some organizations, the BTR life cycle is a one-time planning effort. To achieve true excellence, you must approach it as a *continuous* life cycle. This means you must: 1) embed each of the five processes in BT operations; 2) maintain a current understanding of business context and risk; 2) adjust strategy whenever the business or IT environment changes; 3) update plans as part of change and configuration management and after every test debrief; and 4) exercise and test quarterly or more frequently as the need arises (e.g., before a new app or service is deployed in production). For each process, you must collect appropriate performance metrics (e.g., Balanced Scorecard metrics), report them to both business and technology management leaders on a regular cadence, use them to measure the effectiveness of your team, and, finally, set appropriate targets for improvement for subsequent quarters and years.[14] Without process excellence, technology is irrelevant. Furthermore, as we outsource more and more IT services to cloud and managed service providers, process excellence will be the primary role that I&O will serve in technology management.

SUPPLEMENTAL MATERIAL

Methodology

In the fall of 2013, Forrester Research and the Disaster Recovery Journal (DRJ) conducted an online survey of 66 DRJ members. The survey used a self-selected group of respondents (DRJ members) and is therefore not random. These respondents are more sophisticated than the average. They read and participate in business continuity (BC) and disaster recovery publications, online discussions, etc. They have above-average knowledge of best practices and technology in BC/DR. While nonrandom, the surveys are still a valuable tool in understanding where advanced users are today and where the industry is headed.

ENDNOTES

[1] In late October 2012, Superstorm Sandy barreled through the Caribbean and the eastern US, affecting almost half of the states in the US. The storm left millions without access to basic infrastructure, thousands without homes, and hundreds lost their lives. And for weeks after the storm, thousands of businesses and individuals had no access to power or Internet in some of the densest commercial regions in the US. From a business technology resiliency perspective, many organizations rose to the occasion and weathered the storm with minimal business disruption, while others hit roadblocks and unforeseen challenges. See the April 12, 2013, "Seven Business Technology Resiliency Lessons Learned From Superstorm Sandy" report.

[2] A well-documented strategic plan is imperative because it will help I&O leaders embed and manage BT resiliency across a complex organization, assess and continuously improve the state of BT resiliency, prioritize future projects, and clearly define and communicate I&O's role and responsibility in the organization's broader business continuity and enterprise risk management strategy. See the April 8, 2013, "Elevate Your Business Technology Resiliency Program With An In-Depth Strategic Plan" report and see the October 15, 2012, "Assess The Maturity Of Your Business Technology Resiliency Program" report.

[3] To centralize BCM governance and enforce standards across a complex and geographically distributed organization, you need software; you've needed it for years, and it's time to invest. See the May 26, 2011, "Market Overview: Business Continuity Management Software, Q2 2011" report.

[4] Continual improvement of business continuity programs through benchmarks is important, because in today's digital age, if IT is unavailable, the business is unavailable. See the September 10, 2012, "Benchmark The Performance Of Your Business Continuity Program" report.

[5] Although a business impact analysis (BIA) is a key part of putting together a disaster recovery plan, many companies neglect to conduct one. Forrester believes it's worthwhile to take a step back and conduct a BIA and risk assessment because it provides an opportunity to ask business owners for input into recovery-time and recovery-point objectives. See the July 23, 2010, "Forrester's Business Impact Analysis Template" report.

[6] From understanding comes action. Your risk management efforts up to this point will have yielded a list of concerns; a measure of how much these concerns could affect objectives; and a decision of whether, when, and how to address them. The last step in the risk management process is to act upon this information to make sure your organization takes full advantage of opportunities without exposing itself to unacceptable levels of risk. See the January 16, 2013, "The Risk Manager's Handbook: How To Plan And Execute Appropriate Risk Treatment" report.

[7] Please refer to FEMA reports on declared disasters in the United States. Source: "Disaster Declarations," Federal Emergency Management Agency (http://www.fema.gov/news/disaster_totals_annual.fema); and "Global Survey of Early Warning Systems," The United Nations (http://www.wmo.ch/pages/prog/drr/events/ews_symposium_2006/documents/1.2.%20Global_Survey_EWS.pdf).

[8] Earthquakes, tornadoes, monsoons, hurricanes, flooding, and other severe natural disasters have brought alarming devastation to regions around the world over the past several years. As the human, financial, and ecological toll of these successive events continue, business continuity/disaster recovery (BC/DR) and risk managers want to know what they can learn from these events that can help them better prepare for future disasters. See the July 14, 2011, "Lessons Learned From The 2011 Japanese Crisis" report.

[9] Please refer to the Contingency Planning Guide for Federal Information Systems. Source: National Institute of Standards and Technology (http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf).

[10] The chance that you could successfully recover IT operations without having exercised your DR plans on a regular basis is slim at best. The chance that you could successfully recover and meet your recovery objectives is zero. Yet Forrester finds that exercising DR plans is one area in which many organizations continue to fall short. See the October 26, 2011, "Disaster Recovery Exercises Fall Short Of The Finish Line" report.

[11] Everyone knows you must exercise your business continuity (BC) plans. However, in dozens of inquiries and consulting engagements with enterprise clients each quarter, Forrester finds that BC managers are lucky if they can exercise a portion of a particular BC plan once per year. In fact, we find that BC exercise programs as a whole are quite immature. Common pitfalls are designing unrealistic exercise scenarios, failing to run exercises often enough, and neglecting to integrate with other teams, such as crisis management and IT. See the December 14, 2011, "Stop The Insanity: If You Don't Exercise Your Business Continuity Plans, You Aren't Prepared" report.

[12] Source: Forrester/Disaster Recovery Journal Crisis Communication, Risk Management, And Business Continuity Survey, Q4 2013.

[13] Source: Forrester/Disaster Recovery Journal Business Continuity Preparedness Survey, Q4 2011.

[14] The current state of BTR metrics is unsatisfactory — most programs focus too much on the alphabet soup of recovery time objectives (RTOs) and recovery point objectives (RPOs). As a result, many lose track of critical components of a mature BTR program, such as business sponsor involvement, vetting and testing recovery capabilities, and keeping plans current and relevant. See the April 30, 2012, "Develop Your Business Technology Resiliency Balanced Scorecard" report.

FORRESTER®

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On Infrastructure & Operations Professionals

You are responsible for identifying — and justifying — which technologies and process changes will help you transform and industrialize your company's infrastructure and create a more productive, resilient, and effective IT organization. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« **IAN OLIVER,** client persona representing Infrastructure & Operations Professionals