DOWNLOAD PDF HR GUIDE TO BUSINESS CONTINUITY PLANNING

Chapter 1 : A Guide to Business Continuity Planning

Business Continuity Planning is a proactive planning process that ensures critical services or products are delivered during a disruption. A Business Continuity Plan includes: Plans, measures and arrangements to ensure the continuous delivery of critical services and products, which permits the organization to recover its facility, data and assets.

Communications, transportation, safety and service sector failure Environmental disasters such as pollution and hazardous materials spills Cyber attacks and hacker activity. Creating and maintaining a BCP helps ensure that an institution has the resources and information needed to deal with these emergencies. Creating a business continuity plan A BCP typically includes five sections: BCP Governance Plans, measures, and arrangements for business continuity Readiness procedures Quality assurance techniques exercises, maintenance and auditing Establish control A BCP contains a governance structure often in the form of a committee that will ensure senior management commitments and define senior management roles and responsibilities. The BCP senior management committee is responsible for the oversight, initiation, planning, approval, testing and audit of the BCP. It also implements the BCP, coordinates activities, approves the BIA survey, oversees the creation of continuity plans and reviews the results of quality assurance activities. Senior managers or a BCP Committee would normally: This BCP committee is normally comprised of the following members: Security Officer works with the coordinator to ensure that all aspects of the BCP meet the security requirements of the organization. Business unit representatives provide input, and assist in performing and analyzing the results of the business impact analysis. The BCP committee is commonly co-chaired by the executive sponsor and the coordinator. Identify the mandate and critical aspects of an organization This step determines what goods or services it must be delivered. Information can be obtained from the mission statement of the organization, and legal requirements for delivering specific services and products. Prioritize critical services or products Once the critical services or products are identified, they must be prioritized based on minimum acceptable delivery levels and the maximum period of time the service can be down before severe damage to the organization results. To determine the ranking of critical services, information is required to determine impact of a disruption to service delivery, loss of revenue, additional expenses and intangible losses. Identify impacts of disruptions The impact of a disruption to a critical service or business product determines how long the organization could function without the service or product, and how long clients would accept its unavailability. It will be necessary to determine the time period that a service or product could be unavailable before severe impact is felt. Identify areas of potential revenue loss To determine the loss of revenue, it is necessary to determine which processes and functions that support service or product delivery are involved with the creation of revenue. If these processes and functions are not performed, is revenue lost? If services or goods cannot be provided, would the organization lose revenue? If so, how much revenue, and for what length of time? If clients cannot access certain services or products would they then to go to another provider, resulting in further loss of revenue? Identify additional expenses If a business function or process is inoperable, how long would it take before additional expenses would start to add up? How long could the function be unavailable before extra personnel would have to be hired? Would fines or penalties from breaches of legal responsibilities, agreements, or governmental regulations be an issue, and if so, what are the penalties? Identify intangible losses Estimates are required to determine the approximate cost of the loss of consumer and investor confidence, damage to reputation, loss of competitiveness, reduced market share, and violation of laws and regulations. Loss of image or reputation is especially important for public institutions as they are often perceived as having higher standards. Insurance requirements Since few organizations can afford to pay the full costs of a recovery; having insurance ensures that recovery is fully or partially financed. When considering insurance options, decide what threats to cover. It is important to use the BIA to help decide both what needs insurance coverage, and the corresponding level of coverage. Some aspects of an operation may be overinsured, or underinsured. Minimize the possibility of overlooking a scenario, and to ensure coverage for all eventualities. Document the level of coverage of your institutional policy, and examine the policy for uninsured areas and non specified levels of coverage. Property insurance

may not cover all perils steam explosion, water damage, and damage from excessive ice and snow not removed by the owner. Coverage for such eventualities is available as an extension in the policy. When submitting a claim, or talking to an adjustor, clear communication and understanding is important. Ensure that the adjustor understands the expected full recovery time when documenting losses. The burden of proof when making claims lies with the policyholder and requires valid and accurate documentation. Include an expert or an insurance team when developing the response plan. Ranking Once all relevant information has been collected and assembled, rankings for the critical business services or products can be produced. Ranking is based on the potential loss of revenue, time of recovery and severity of impact a disruption would cause. Minimum service levels and maximum allowable downtimes are then determined. Identify dependencies It is important to identify the internal and external dependencies of critical services or products, since service delivery relies on those dependencies. Internal dependencies include employee availability, corporate assets such as equipment, facilities, computer applications, data, tools, vehicles, and support services such as finance, human resources, security and information technology support. External dependencies include suppliers, any external corporate assets such as equipment, facilities, computer applications, data, tools, vehicles, and any external support services such as facility management, utilities, communications, transportation, finance institutions, insurance providers, government services, legal services, and health and safety service. These plans and arrangements detail the ways and means to ensure critical services and products are delivered at a minimum service levels within tolerable down times. Continuity plans should be made for each critical service or product. Mitigating threats and risks Threats and risks are identified in the BIA or in a full-threat-and-risk assessment. Moderating risk is an ongoing process, and should be performed even when the BCP is not activated. For example, if an organization requires electricity for production, the risk of a short term power outage can be mitigated by installing stand-by generators. Another example would be an organization that relies on internal and external telecommunications to function effectively. Communications failures can be minimized by using alternate communications networks, or installing redundant systems. Analyze current recovery capabilities Consider recovery arrangements the organization already has in place, and their continued applicability. Include them in the BCP if they are relevant. Create continuity plans Plans for the continuity of services and products are based on the results of the BIA. Ensure that plans are made for increasing levels of severity of impact from a disruption. If water rises to the first floor, work could be moved to another company building or higher in the same building. If the flooding is severe, the relocation of critical parts of the business to another area until flooding subsides may be the best option. Another example would be a company that uses paper forms to keep track of inventory until computers or servers are repaired, or electrical service is restored. For other institutions, such as large financial firms, any computer disruptions may be unacceptable, and an alternate site and data replication technology must be used. The risks and benefits of each possible option for the plan should be considered, keeping cost, flexibility and probable disruption scenarios in mind. For each critical service or product, choose the most realistic and effective options when creating the overall plan. Response preparation Proper response to a crisis for the organization requires teams to lead and support recovery and response operations. Team members should be selected from trained and experienced personnel who are knowledgeable about their responsibilities. For the teams to function in spite of personnel loss or availability, it may be necessary to multitask teams and provide cross-team training. There are three types of alternate facility: Cold site is an alternate facility that is not furnished and equipped for operation. Proper equipment and furnishings must be installed before operations can begin, and a substantial time and effort is required to make a cold site fully operational. Cold sites are the least expensive option. Warm site is an alternate facility that is electronically prepared and almost completely equipped and furnished for operation. It can be fully operational within several hours. Warm sites are more expensive than cold sites. Hot site is fully equipped, furnished, and often even fully staffed. Hot sites can be activated within minutes or seconds. Hot sites are the most expensive option. When considering the type of alternate facility, consider all factors, including threats and risks, maximum allowable downtime and cost. For security reasons, some organizations employ hardened alternate sites. Hardened sites contain security features that minimize disruptions. Hardened sites may have alternate power supplies; back-up generation capability;

high levels of physical security; and protection from electronic surveillance or intrusion. Readiness procedures Training Business continuity plans can be smoothly and effectively implemented by: While exercises are time and resource consuming, they are the best method for validating a plan. The following items should be incorporated when planning an exercise: Goal The part of the BCP to be tested. Objectives The anticipated results. Objectives should be challenging, specific, measurable, achievable, realistic and timely. Scope Identifies the departments or organizations involved, the geographical area, and the test conditions and presentation. Artificial aspects and assumptions Defines which exercise aspects are artificial or assumed, such as background information, procedures to be followed, and equipment availability. Participant Instructions Explains that the exercise provides an opportunity to test procedures before an actual disaster. Exercise Narrative Gives participants the necessary background information, sets the environment and prepares participants for action. It is important to include factors such as time, location, method of discovery and sequence of events, whether events are finished or still in progress, initial damage reports and any external conditions. Communications for Participants Enhanced realism can be achieved by giving participants access to emergency contact personnel who share in the exercise. Messages can also be passed to participants during an exercise to alter or create new conditions. Testing and Post-Exercise Evaluation The exercise should be monitored impartially to determine whether objectives were achieved. Debriefing should be short, yet comprehensive, explaining what did and did not work, emphasizing successes and opportunities for improvement. Participant feedback should also be incorporated in the exercise evaluation. Exercise complexity level can also be enhanced by focusing the exercise on one part of the BCP instead of involving the entire organization. It should also uncover which aspects of a BCP need improvement. Continuous appraisal of the BCP is essential to maintaining its effectiveness. The appraisal can be performed by an internal review, or by an external audit.

Chapter 2 : Business Continuity Checklist | Business Continuity Planning Checklist

This bar-code number lets you verify that you're getting exactly the right version or edition of a book. The digit and digit formats both work.

The implementation phase involves policy changes, material acquisitions, staffing and testing. Testing and organizational acceptance[edit] The purpose of testing is to achieve organizational acceptance that the solution satisfies the recovery requirements. Plans may fail to meet expectations due to insufficient or inaccurate recovery requirements, solution design flaws or solution implementation errors. Crisis command team call-out testing Technical swing test from primary to secondary work locations Technical swing test from secondary to primary work locations Application test Business process test At minimum, testing is conducted on a biannual schedule. The book Exercising for Excellence, published by The British Standards Institution identified three types of exercises that can be employed when testing business continuity plans. Tabletop exercises[edit] Tabletop exercises typically involve a small number of people and concentrates on a specific aspect of a BCP. They can easily accommodate complete teams from a specific area of a business. Another form involves a single representative from each of several teams. Typically, participants work through simple scenario and then discuss specific aspects of the plan. For example, a fire is discovered out of working hours. The exercise consumes only a few hours and is often split into two or three sessions, each concentrating on a different theme. Medium exercises[edit] A medium exercise is conducted within a "Virtual World" and brings together several departments, teams or disciplines. It typically concentrates on multiple BCP aspects, prompting interaction between teams. The scope of a medium exercise can range from a few teams from one organisation co-located in one building to multiple teams operating across dispersed locations. The environment needs to be as realistic as practicable and team sizes should reflect a realistic situation. Realism may extend to simulated news broadcasts and websites. A medium exercise typically lasts a few hours, though they can extend over several days. They typically involve a "Scenario Cell" that adds pre-scripted "surprises" throughout the exercise. Complex exercises[edit] A complex exercise aims to have as few boundaries as possible. It incorporates all the aspects of a medium exercise. The exercise remains within a virtual world, but maximum realism is essential. This might include no-notice activation, actual evacuation and actual invocation of a disaster recovery site. While start and stop times are pre-agreed, the actual duration might be unknown if events are allowed to run their course. Maintenance[edit] Biannual or annual maintenance cycle maintenance of a BCP manual is broken down into three periodic activities. Confirmation of information in the manual, roll out to staff for awareness and specific training for critical individuals. Testing and verification of technical solutions established for recovery operations. Testing and verification of organization recovery procedures. Issues found during the testing phase often must be reintroduced to the analysis phase. Like most business procedures, business continuity planning has its own jargon. Organisation-wide understanding of business continuity jargon is vital and glossaries are available.

Chapter 3 : 4 Ways to Create a Business Continuity Plan - wikiHow

Business continuity is an on-going process to help ensure that the necessary steps are taken to identify the impact of potential losses and maintain viable recovery strategies.

Chapter 4 : 8 tips for building a business continuity plan | calendrierdelascience.com

A business continuity plan to continue business is essential. Development of a business continuity plan includes four steps: Conduct a business impact analysis to identify time-sensitive or critical business functions and processes and the resources that support them.

Chapter 5 : HR-Guide Homepage

DOWNLOAD PDF HR GUIDE TO BUSINESS CONTINUITY PLANNING

Participate in your business continuity planning process and help your business define parts of your plan, such as Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). Augment your IT staff during critical events by leveraging our IT staff, who are available 24x7x

Chapter 6 : Business Continuity Planning and Disaster Recovery Online Guide

A beginners guide to the Business Continuity Planning process Posted by Inoni on June 10, Almost every prudent business, large or small sees wisdom in buying some level of business insurance.

Chapter 7 : Business continuity planning - Wikipedia

This guide consists of two sections. The first section will help guide you in the creation of a business continuity plan. It includes helpful information as well as useful worksheets to help collect vital information.