Contingency planning: Riding the storm

Posted by **Emily Hough** on **11th September 2015** at **09:30am**

How a government agency adapts and responds to disasters determines its ability to continue to fulfil its mission and provide essential services, says Gary Villeneuve. Good contingency planning meets that need.

Photo: Zackery Blanton / 123RF

Contingency planning includes continuity plans for mission-essential functions and critical processes for which a government agency or organisation is responsible. Development of contingency and continuity plans requires a disciplined approach so the plans can be managed effectively.

Before developing any contingency and continuity plan, government agencies should initiate a Continuity of Operations, or COOP programme, outlining the steps needed for plan development and management. There are several sound reasons for this, including: Protecting personnel; protecting essential facilities and resources; achieving a timely and orderly recovery; resuming full service to recipients; serving the public interest; and complying with agency directives, regulations and requirements.

COOP programme initiation involves leadership and management commitment, staffing personnel to perform the duties of contingency and continuity planning and execution, identifying facilities in which tasks can be carried out, and communicating information to stakeholders. Management commitment involves approving a budget to achieve objectives and complete required tasks.

Establish the need for the programme within the organisation and its components from understanding the entity's risks and vulnerabilities through development of resilience strategies and response, restoration and recovery plans. The organisation must support the programme with funding and build the programme framework.

After establishing a COOP programme, government organisations should conduct a risk assessment and once threats, their associated risks and vulnerabilities have been identified and prioritised, controls and countermeasures should be identified and installed to reduce, or mitigate, organisational exposure and the cost to implement such controls evaluated. Once identified, threats and vulnerabilities will be assessed as to the likelihood they would occur and the potential level of impact that would result.

The next step is a business process analysis, or BPA, and a business impact analysis (BIA). These provide information upon which continuity strategies and plans can be built. The processes involve collecting information through questionnaires, interviews, meetings and other sources from key personnel and managers within the agency or organisation.

The combination of the BPA and BIA will determine mission function and process criticality, including critical time periods, as well as identifying interdependencies between functions and processes. It will assess the impact of potential disruptions over time and identify the critical resources needed for recovery, including vital records. It will also determine the recovery time objectives (RTO) and recovery point objectives (RPOs) for each function and process, and determine legal and regulatory requirements. It is important to measure and assess the financial, operational, customer, regulatory and/or reputational impacts and determine the RTO and RPO for each of the organisation's functions and processes.

After the risk assessment, BPA and BIA are developed, government agencies and their subordinate activities should develop predetermined sets of instructions or procedures describing how mission-essential functions and critical processes will be continued or recovered within documented RTOs and sustain those functions and processes affected by disaster event(s) for some period of time before returning to normal.

Recommended strategies must be approved, funded and meet both the RTO and RPO identified in the BPA and BIA. A cost benefit analysis on the recommended strategies should be performed to align the cost of implementing the strategy against the assets at risk.

However, unless continuity plans are tested and exercised, the agency cannot be sure it will be able to provide essential services or reconstitute its mission essential functions and critical processes should a catastrophe occur. The primary purpose of performing exercises and tests is to identify deficiencies in COOP plans. Proper plan maintenance through change management also matures the continuity programme.

Implement a regular exercise schedule to establish continuity and recovery processes throughout the organisation. Use change management to track and document the continuity and recovery processes readiness, enable continuous improvement to these capabilities, and ensure that plans remain current and relevant. Establish an audit process in order to validate plans, ensure they are complete and accurate and that they comply with organisational goals, regulations, and industry standards as needed.

Prioritising, evaluating and implementing risk reduction, or mitigation, controls and countermeasures are an integral part of the risk management process. The primary purpose of risk mitigation is to reduce the consequences of an event before it occurs. This is also referred to as risk treatment.

The Emergency Response Plan documents how the organisation will respond to disaster events in a co-ordinated,

timely and effective manner to address life safety and stabilisation of emergency situations until the arrival of trained or external first responders. The Business Recovery/Continuity Plan is a set of documented processes and procedures, which will enable the entity to continue or recover time sensitive processes to the minimum acceptable level within the timeframe acceptable to the entity.

Before implementing controls and undertaking risk treatment, the organisation's risk profile, risk appetite and risk tolerance must be established. A risk profile is the list of threats, along with their associated risks and vulnerabilities. Risk appetite is the total amount of risk an organisation is prepared to accept or tolerate, while risk tolerance is an organisation's readiness to bear risk after risk treatments have been established in order to achieve its objectives. To better understand mitigation, we must know what a control, or counter-measure, is and which controls are appropriate for various threats.

Emergency management is the responsibility of external agencies, government agencies and public authorities, complying with appropriate laws that relate to emergency response. When a disaster occurs, government agencies typically establish emergency operations centres, or EOCs, from which strategic decisions are made and all activities of an incident are directed, co-ordinated and monitored.

Subordinate command centres also can be established to manage the tactical operations needed to respond to the incident. These are located in somewhat close proximity to the event but outside the immediate affected area, where the tactical response, recovery and restoration activities are directed. There may be more than one command centre for each event reporting to a single EOC.

In addition, an incident command post, or ICP, can be established at or in the immediate vicinity of the incident site to conduct direct, on-scene control of tactical operations. The ICP reports to the command centre, which reports to the EOC. This overall hierarchy enables co-ordination of crisis response in an effective, timely manner, to respond and reduce damage to the community. This also involves strategic direction of the private sector's response, while the public sector's primary role in an emergency is to stabilise the event, provide the life safety response and maintain control of the event until it is declared over.

Private sector operators need to understand what system they use to manage events, and understand their role in an event. They should also build relationships with government authorities before a disaster occurs. One good way to achieve this is to take part in exercises with government agencies such as Fire or Police Services. Such relationships will provide them access to the resources needed to respond and recover more quickly, access to external information and an improved connection with stakeholders.

These steps are an overview of DRI International's Professional Practices, and following them will put your organisation on the path to continuity and resiliency. It is also important to remember, "A plan not exercised is not a plan".

Author

Gary Villeneuve is Director of Education at the Disaster Recovery Institute International. This article appears in CRJ 11:1, click here for more details.