

## CONTINGENCY PLANNING & RISK MANAGEMENT PROCESS

Risk management encompasses a broad range of activities to identify, control, and mitigate risks to an IT system. Risk management activities from the IT contingency planning perspective have two primary functions. First, risk management should identify threats and vulnerabilities so that appropriate controls can be put into place to either prevent incidents from happening or to limit the effects of an incident. These security controls protect an IT system against three classifications of threats—

- **Natural**—e.g., hurricane, tornado, flood, and fire
- **Human**<sup>3</sup>—e.g., operator error, sabotage, implant of malicious code, and terrorist attacks
- **Environmental**—e.g., equipment failure, software error, telecommunications network outage, and electric power failure.

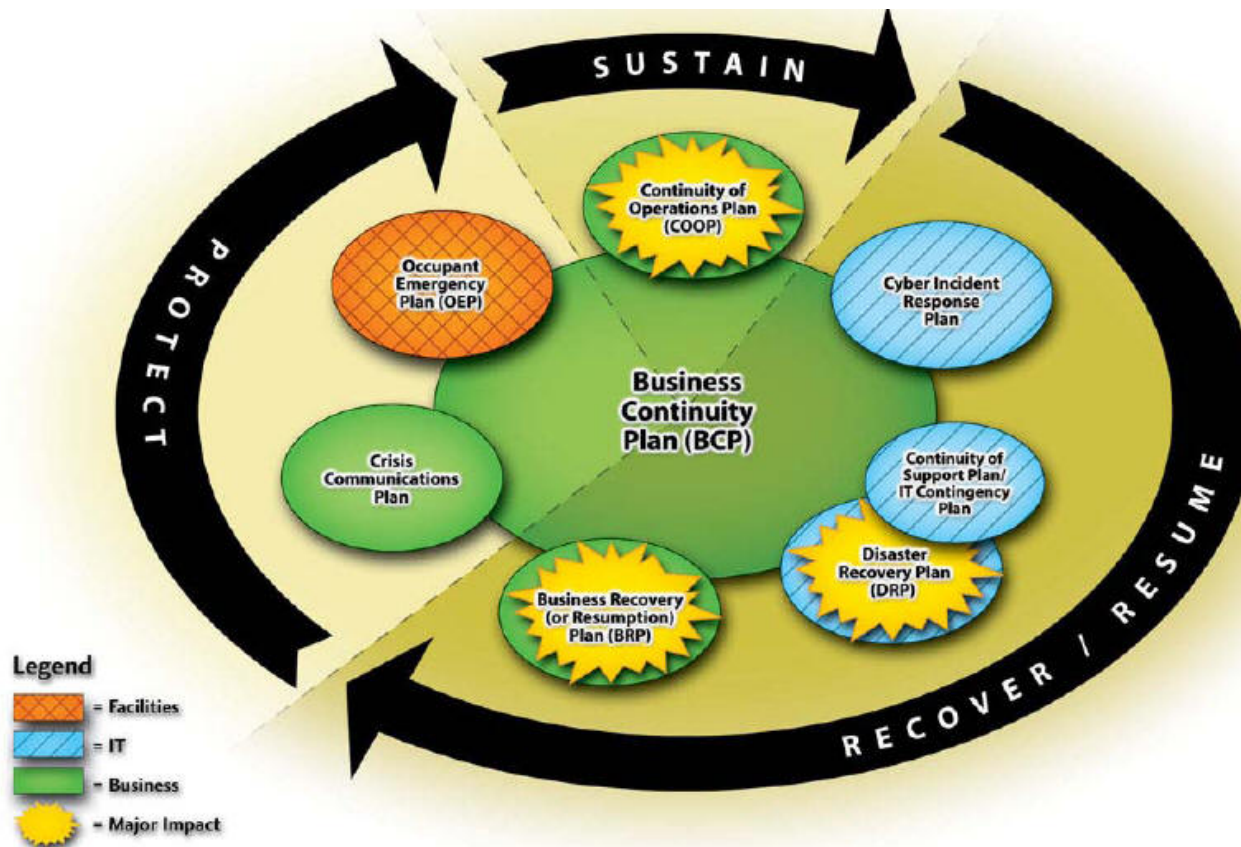
Second, risk management should identify residual risks for which contingency plans must be put into place. The contingency plan, therefore, is very closely tied to the results of the risk assessment and its mitigation process. Figure 2-1 illustrates the relationship between identifying and implementing security controls, developing and maintaining the contingency plan, and implementing the contingency plan once the event has occurred.



Figure 2-1 Contingency Planning as an Element of Risk Management Implementation

Plan	Purpose	Scope
Business Continuity Plan (BCP)	Provide procedures for sustaining essential business operations while recovering from a significant disruption	Addresses business processes; IT addressed based only on its support for business process
Business Recovery (or Resumption) Plan (BRP)	Provide procedures for recovering business operations immediately following a disaster	Addresses business processes; not IT-focused; IT addressed based only on its support for business process
Continuity of Operations Plan (COOP)	Provide procedures and capabilities to sustain an organization's essential, strategic functions at an alternate site for up to 30 days	Addresses the subset of an organization's missions that are deemed most critical; usually written at headquarters level; not IT-focused
Continuity of Support Plan/IT Contingency Plan	Provide procedures and capabilities for recovering a major application or general support system	Same as IT contingency plan; addresses IT system disruptions; not business process focused
Crisis Communications Plan	Provides procedures for disseminating status reports to personnel and the public	Addresses communications with personnel and the public; not IT focused
Cyber Incident Response Plan	Provide strategies to detect, respond to, and limit consequences of malicious cyber incident	Focuses on information security responses to incidents affecting systems and/or networks
Disaster Recovery Plan (DRP)	Provide detailed procedures to facilitate recovery of capabilities at an alternate site	Often IT-focused; limited to major disruptions with long-term effects
Occupant Emergency Plan (OEP)	Provide coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat	Focuses on personnel and property particular to the specific facility; not business process or IT system functionality based

## Interrelationship of Emergency Preparedness Plans



## Contingency Planning Process

