CHAPTER 1

Business Continuity Management Plan

The incident management plan (IMP) is a detailed component of a Business Continuity Management (BCM) Plan. Also known as the enterprise resilience, emergency preparedness, or risk management plan, it forms the advance planning aspects that enable the initial crisis response activities to be conducted in a prearranged and organized fashion. The IMP is designed to support business continuity and incident recovery at the early stages, meeting immediate event response needs as resources are mobilized and more mature and comprehensive management measures are brought into play. The IMP can bridge, or be part of, more detailed crisis response plans such as evacuation management, disaster response, and reputational recovery, as well as dealing with kidnap and ransom situations and pandemics. However, these stand-alone plans are often better served as comprehensive components within the overall Business Continuity Management Plan (as they will likely be more oriented to specific divisions, fields, or regions), whereas the IMP addresses more common and generic risk types that the organization might face at the outset of a crisis event. The IMP at the basic level supports immediate tactical considerations and management functions, rather than long-term risk management and business recovery needs. Where feasible, the company should seek to transfer decision making to the lowest levels possible for the initial response requirements, as this will strengthen and empower local managers to contribute effectively to the management and early resolution of a crisis event.

Business Continuity Planning Terms

- Contingency planning and crisis management
- Enterprise resilience
- Emergency preparedness
- Enterprise risk management
- Emergency management
- Critical situations management

For the purposes of this book, incident management focuses not on the strategic, specialist, or sustained response measures, but on more granular and tactical support mechanisms that are the precursors to more complex and corporate-driven crisis

management and business recovery policies and plans: *the first 24 to 72 hours of an emergency.* This book touches on the broader aspects of risk management in order to support the reader in placing the IMP within an understandable context. However, the book is principally designed to discuss the first stages of crisis response where incident management will play an active part in bringing an emergency situation under control, as well as feeding crucial information to company officers. The IMP is a tool for a wide spectrum of users, not only security professionals or corporate leadership. As such, the IMP supports local management in collating accurate information and following simple response guidelines to reduce the initial impacts of an emergency event, bringing control to a situation and further mitigating the risks that could escalate out of control from a problem, or be created as secondary or peripheral effects as a result of the initial crisis event. The IMP in these terms is also a short-term measure, allowing a degree of organized control to be implemented while the company mobilizes resources and specialists during the early stages of an emergency.

Companies should be aware that the social fabric of a culture or an area can be quickly undermined by a crisis situation, resulting in unique and challenging risks to commercial organizations, their employees (and families), facilities, and business activities. Even within Western countries, the speed at which deteriorations in governance, basic amenities, and societal rules can be surprising. The implications can be widespread and catastrophic, or localized and disruptive. Crisis events may result from a natural disaster: a flood, earthquake, hurricane, or pandemic. They may result from widespread civil disorder: a coup, political instability, insurgency, or war. Or a crisis event may be localized: a riot following a football match, aggressive measures over farming disputes, fuel shortages, a focused labor dispute issue, or directed attacks against individuals, groups, or facilities.

The following list illustrates some macro-level considerations companies should incorporate into their strategic planning for crisis management:

- **Governance.** The loss of governmental control and policing authority can be swift and widespread. Government offices may be directly affected or overwhelmed by a crisis event, and officials may not have the knowledge, capacity, or resources to quickly support the affected populace. Government offices dedicated to dealing with a crisis situation may also be undermined as personnel respond to personal emergencies or to care for families, diminishing a government's expected capacity to respond to a crisis effectively.
- **Social Fabrics.** The social norms that regulate our societies can be quickly lost or undermined as the effectiveness of governance is diminished. Rioting, thefts, looting, and other social crimes can quickly spread to otherwise law-abiding sections of the community. This is a cyclic effect and can create a further loss of governance which might exacerbate a crisis and add additional elements of risk to the original crisis event.
- **Utilities.** Common utilities and services can be disrupted, such as power, water, sewage, and communications, during a crisis. Basic amenities like food availability, financial services, and fuel provisions can also be affected. Modern cultures are not best engineered to weather a loss of power or disruptions to food, fuel supplies, or utilities, and often struggle to manage if common services are disrupted, and such losses can also result in secondary crisis events.

- **Movement.** Movement can be affected by crisis situations, whether due to man-made risks presented by hostile or disruptive groups, or due to damaged infrastructures or the unavailability of fuel or power supplies. This can affect every aspect of emergency management, from those dealing with emergencies at the point of crisis to those attempting to respond in support of the emergency or evacuate from an affected area.
- **Critical Services.** Critical services, such as fire response, medical provisions, and health care, or critical infrastructure power and utilities can be seriously undermined with the loss of basic utilities, undermining the ability for such groups to respond to or support an affected population. Infrastructure damage and affected supply chains of critical materials or resources can quickly devalue otherwise effective critical service providers.
- **Communications.** Communication mediums may be affected by a crisis event disrupting or preventing the effective passage of information and instructions which might support an understanding of the crisis event, as well as the effective response to an emergency. Communication systems may be damaged, or overwhelmed by a surge of use. Often voice mediums are lost before text and this can affect both government entities' ability to mobilize and respond to a crisis, as well as a commercial organization's respond measures.

Crisis Definitions

A crisis is (1) an unstable condition, as in political, social, or economic affairs, involving an impending abrupt or decisive change, or (2) an abnormal or unique event that threatens groups or individuals, as well as their goals and enterprises, through disruptive or harmful effects.

A crisis event can also be considered in terms of the micro- and macro-level crisis. The micro crisis is the point of the event: a collapsed building, fuel leak, or roadside fatality. The macro crisis consists of all of the risks that originate and ripple outward from that event: threats posed to surrounding buildings, recovering trapped persons, bringing control to the oil leak, dealing with the media, and reducing reputational and liability risks. In these terms, the IMP typically focuses on the micro-level crisis: the event itself. The IMP does, however, play a fundamental role in supporting the company in dealing with macro-level considerations and threats. Therefore, the IMP may be considered the first of many steps within a broader crisis response plan, acting as a precursor to the fuller crisis response measures being implemented by the company, as well as the transition point at which a company goes from managing the incident to controlling the effects of the wider crisis. This is a subjective delineation and will of course be influenced by the nature of the event, the composition of different management teams involved within the emergency, and the operating environment in which a company is performing work. An effectively designed and implemented IMP reflects the level of effort a company invests into ensuring the safety and welfare of its employees, protecting its business interests and brand value, and maximizing operational productivity through

pragmatic contingency planning measures that enable effective, immediate, interim, and long-term crisis response mechanisms and methodologies to be implemented.

Given the ease at which organizational control and governmental support can be lost during a crisis, companies should seek to design and resource a degree of self-reliance within their crisis planning that takes into consideration these factors, while still leveraging and exploiting external governmental and other resources to support their response measures and capabilities.

Crisis Management

For the management of risk within a nonspecialized industry or more tangible fields such as construction, development, power and water, fuels, maritime and air, consulting, and training, the company's or its security vendor's crisis response team typically comes from a military or law enforcement background where the concept of incident management and crisis response has been an integrated aspect of their careers. In addition, subject matter experts within areas such as health and safety, engineering, administration, and legal considerations will also support critical crisis response decision making. Where risk elements are more market sector focused, such as business, financial investments, and mergers and acquisitions, more specialist risk managers may be required within defined fields such as information technology (IT), investments, and business intelligence. Typically, outside of pure investment and business risk areas, the initial point of a crisis event will be operationally oriented and occur at a point or location away from such expertise, although more nebulous risks will result from a physical event. The IMP should be designed to withstand a lack of experience or knowledge by users who operate outside of the risk and security management field. It should be a pragmatic, simple, and user-friendly tool; and the design and testing of such a plan should incorporate users as well as managers and specialists in order to ensure that plans are logical and unambiguous, reflect the operating conditions, and, most importantly, are implementable and understood.

Companies should seek to leverage the capabilities, knowledge, and resources of both in-house experience and knowledge, as well as that of their security vendors to provide, supplement, or augment their business continuity policies and plans. When operating within more challenging environments where the probability or impact of risk is higher, companies should consider the value of transferring both the risks and the resources required for establishing the Business Continuity Management Plan, as well as its various subcomponents such as the IMP and evacuation plans, to their security vendors or outsourced consultants in order to offset both risk exposure and development effort. That said, integration for any crisis planning should be established to blend outsourced and company requirements and activities at all levels. The scope of work for any security contract in such regions should include clear requirements for the vendor to provide contingency plans and crisis management protocols as part of the overall service-level agreement. While the company can never fully defer crisis management responsibility to a subcontractor, corporate and field risk managers can establish policies and procedures by which much of the burden of dealing with a crisis event can be transferred onto an appropriate vendor, while strategic decision-making authorities are retained by the company, as well as corporate risk response measures. These agreements should be understood and the

plans and responses clearly articulated and practiced in order to ensure that the most effective risk management approach is in place.

The Value

The investment in terms of time, money, and resources in developing a Business Continuity Management Plan can be seen both in tangible terms of safeguarding personnel and facilities, as well as in often bringing less visible or hard values and benefits to the company, such as increased profits and productivity, market confidence, reputational protection, and employee morale. Business Continuity Management Plans can provide companies greater supply chain assurance; be a market differentiator in terms of effectiveness, agility, and the overall competitive value; and often enable the company to identify, understand, and offset risks prior to their occurrence, as well as perhaps operate within business environments in which they would be otherwise prevented from engaging. Such focus can also be migrated to vendors, ensuring that their approach to business resilience best supports the company, and can also assure investors or clients that the company can weather a crisis effectively—without unduly disrupting business services or operational delivery. A Business Continuity Management Plan can support the company in winning as well as undertaking work through the alignment of risks to business interests and activities, as well as reducing insurance premiums and liability exposure.

What Is Risk Management?

- A system that defines an organizational structure, as well as team roles and responsibilities, to enable a company to react to situations ahead of an emergency.
- A bridge between risk mitigation (business protection), risk management (business resilience), and crisis recovery (business resumption)
- A holistic solution meeting the requirements of all corporate needs and activities, whether related to brand, operations, reputation, or ethos.
- A tool that helps companies negotiate fluid and challenging risk environments, effectively dealing with unpredictable events.
- An insurance mechanism that supports business continuity and recovery when risk mitigation measures fail.

Risk management should be considered a supporting element of business development and operational conduct, regardless of the industry sector or geographic region a company might operate in. It should be considered best practice for companies, safeguarding both corporate and employee interests through well-developed policies, procedures, and plans. The following summarizes some of the benefits that the development of a Business Continuity Management Plan may bring to companies or groups:

- Establishes a corporate agenda and strategic approach.
- Brings awareness and understanding of corporate risks and liabilities.
- Establishes a culture that embodies a common vision and taxonomy for risk.

- Supports better business planning and practices.
- Enhances business discipline and internal controls.
- Protects directors and officers against liability charges and claims.
- Ensures informed decision making to strengthen strategic plans and responses.
- Aligns business with risk management to ensure effective business.
- Reduces reputational and liability risks, and protects brand and investor confidence.
- Protects business activities, resources, and personnel.
- Strengthens business continuity and recovery—improving productivity and profit levels.
- Demonstrates duty of care and sound management practices.
- Reduces insurance premiums and liability claims.
- Improves management and employee confidence and morale.
- Ensures the identification and best use of organic and external resources.
- Provides an evidence chain for investigations and audits.
- Meets industry, governmental, and other regulatory requirements.
- Defines the business strategy, including expansion, new market entry, and downsizing.

The value of developing an effective Business Continuity Management Plan, as well as an accompanying IMP, is illustrated in Exhibit 1.1. It highlights how enterprise resilience and recovery measures can:

- Map risks and guide management responses.
- Protect the company's business and corporate interests.

EXHIBIT 1.1 The Value of Business Continuity Management Plans

- Bring order out of chaos in order to depict a true reflection of an organization's ability to deal with a crisis.
- Provide confidence to managers, employees, clients, and investors.
- Integrate recovery measures across disparate and dispersed organizations.
- Leverage organic and external resources to manage and respond to crises.
- Increase profits and productivity, and reduce costs and liabilities.
- Protect facilities, resources, and human life.
- Meet specific regulatory and industry standards.

A well-resourced Business Continuity Management Plan will also include forms of information or advisory feeds, whether intelligence or environmental or political scanning, in order to ensure that crisis management policies and plans are triggered prior to an event occurring. Such measures will ensure that the plan, or parts of it, are set in motion before the event occurs (i.e., warning of localized flooding, notifications of civil gatherings, and so on). Contingency planning and crisis response investment in terms of money, time, and resources should be considered a fundamental aspect of sound business practice, not a cost center. While difficult to quantify in terms of cost savings, business resilience statistically increases long-term business productivity and operational recovery from crisis situations and should be considered a central aspect of corporate strategic policy and planning functions.

Common Failings

Designing and maintaining a Business Continuity Management Plan can be fraught with problems and can often result in a significant waste of time, resources, and energy in the creation of policies and plans that quickly lose their value and applicability in terms of supporting the company's strategic and tactical interests. Plans are also frequently prepared at significant cost, only to then be ignored, be poorly distributed, or be underutilized during an emergency. It is therefore useful to understand the common failure points in the development and utilization of such plans in order to design and sustain a business continuity architecture that is created—from the outset—to meet the group's long term needs, and that gains management buy-in, is kept current and applicable, and is embraced and understood by the users and stakeholders in order to be effective. The following outlines some key areas in which Business Continuity Management Plans often fall short of potential success:

- **Management Support.** A Business Continuity Management Plan that lacks high-level support is likely to fail from the outset. Corporate leadership needs to fully embrace the value of developing such policies and plans and has to ensure that different company divisions are supportive both of the strategic corporate requirements, as well as their individual areas of group interest. Support should cascade from the top downward in order for plans to be successful. Clear directives should support the plan, ensuring that each group and individual adheres to corporate policy.
- **Ownership.** Ownership of the plans should be established to ensure that participants understand and are accountable for their part within a Business Continuity Management Plan. In addition, a sensible appreciation of who should own certain aspects of the plan should be evaluated, with appropriate managers being empowered to develop, maintain, and manage elements which best

reflect their areas of expertise. Company politics should not drive ownership issues—functional capability should be the defining factor.

- **User Buy-In.** The user audience must also be supportive of the Business Continuity Management Plan. Otherwise, the value of application will be undermined, local managers will be prone to use their own approaches and methodologies, and the ability of users to apply the plan's principles and guidelines during an emergency will be hampered by a lack of awareness, understanding, and enthusiasm for the Business Continuity Management Plan. Seeking user buy-in from the outset will ensure the plan reflects the user and stakeholder needs, and so encourage their support and active participation.
- **Structure and Design.** Often plans are designed that are cumbersome, confusing, and difficult to maintain. Consistency of design and structuring is often quickly lost, and individual divisions or regions are prone to developing their own unique approaches, which can undermine the plan, create confusion, and result in redundancy—or at worst, lead to erroneous directives and guidelines that increase the potential threats. Plans should be designed to be simple, efficient, and easy to maintain or adapt. Consistency in layout, content matter, and generic directives should not prevent regional or activity-specific requirements to be met, but will ensure a clear and logical format for approach.
- **Applicability.** Plans can quickly become redundant as personnel change over, the threat environment shifts, and business activities progress. The structuring and design of plans can make sustainability of plans difficult, causing plans to rapidly become inaccurate or completely redundant—placing the company at risk, as well as incurring unnecessary costs. Plans should be designed in a manner that allows live sections to be easily updated, with static sections to remain constant where applicable. The use of supporting tables, diagrams, and other out-of-plan data feeds will help satisfy this requirement. Plans should have periodic reviews to ensure that adjustments are made and the plans are updated using internal projects as well as corporate quality assurance mechanisms.
- **Training and Education.** The plan is only as good as the users who implement the policies and procedures within it. A failure to adequately advise, train, and rehearse personnel will significantly devalue the Business Continuity Management Plan, making its use disjointed, difficult, and confusing during an emergency. Companies must budget time, resources, and capital to ensure that managers and personnel are educated as to the plan's function, how it will be employed, as well as how to support its development and maintenance.
- **Leveraging Resources.** Business Continuity Management Plans should seek to leverage organic as well as external resources as efficiently and effectively as possible. Often plans fail to capitalize on the raft of support that is available, diminishing potential value as well as incurring unnecessary costs and risks to the company. Plans should be aligned to all possible resources available at corporate, country, and project levels.
- **Accessibility and Maintenance.** Often risk and crisis policies and plans are not accessible to the various users and stakeholders, and as such changes are difficult to undertake and track. Version control of policies and quality assurance can be problematic. Hosting policies and plans on web-based systems can support accessibility as well as the use of a central document to support version control management.

The development of a clear corporate agenda and well-structured goals prior to work commencing on the Business Continuity Management Plan will enable its design, development, and ultimately its sustainment to be achieved more effectively, and with least frustration. The plan should be considered a living and pan-organizational tool that requires group support and buy-in in order to be successful. Time spent on planning is seldom wasted, and companies should develop frameworks for their objectives and requirements fully before commencing work.

Business Continuity Goals

The veneer of safety and security, and indeed in some cases civilization, can be quickly stripped away during, or following, an emergency situation. Common social norms may be temporarily suspended, and governance and basic amenities may be disrupted—leading to unique and challenging risks for individuals and organizations. Companies should therefore have clear goals when designing a Business Continuity Management Plan, seeking to meet strategic, operational, and tactical needs. Considerable time and investment is often wasted through a poorly planned, structured, and implemented approach to designing and implementing Business Continuity Management Plans. Business continuity can be broken into three main areas:

1. **Contingency Planning.** Seeking to avoid a crisis through risk mitigation, as well as preparing for a crisis through the development of plans, agreements, and policies.
2. **Crisis Management.** Utilizing preestablished contingency plans practically in order to manage a crisis event most effectively.
3. **Recovery.** Utilizing preestablished contingency plans to quickly and effectively recover from a crisis and resume operations.

Alternatively, Business Continuity Management can be reflected in the three R's, Ready for an emergency, Response to an emergency, and Risk recovery. In order to be most effective, the Business Continuity Management Plan should address the following objectives as a guiding framework when developing such policies and plans:

- **Intelligent.** The Business Continuity Management Plan and associated policies, protocols, and plans reflect all layers and levels of need. They take into account the corporate ethos, strategic goals and agendas, shareholder interests and perceptions, marketplace and risk environment, as well as individual programmatic issues, organizational structures, cultural influences, resource limitations, and teammates' and vendor's interests.
- **Persuasive.** The Business Continuity Management Plan (where possible and appropriate) gains buy-in throughout the management and user and stakeholder population and is integrated and embraced throughout the group. Integration also occurs with supporting or leveraged agencies and organizations to make the Business Continuity Management Plan operate seamlessly with both internal and external groups.
- **Transparent.** The organizational structure, roles, and responsibilities, as well as communication and decision-making authorities and practices, should be transparent to all managers and users in order for the plan to be effective.

Elements of the plan should also be shared with external groups who might be stakeholders or who might be expected to perform specific functions during a crisis event.

The following are four recommended characteristics that form the basis for the effective development of a Business Continuity Management Plan:

1. **Comprehensive.** Establishes contingency measures that meet the holistic threats facing a company and its activities, and manages the entire life cycle of a crisis.
2. **Integrated.** Unites all appropriate organizational divisions, external agencies, vendors, teammates, and other parties into an integrated system.
3. **Flexible.** Can match the tempo and direction of a fluid business and risk environment, allowing all threats to be appropriately mitigated or managed.
4. **Benchmarked.** Is developed using mature and quantified (where possible) evaluations of the risk natures and probable impacts a company might face.

Defining a Crisis

The term *crisis* is subjective and fluid. It is important when developing a Business Continuity Management Plan, with its various components (including the IMP), to first define what is considered a commonplace problem against what might be considered significant enough to warrant the title "crisis." Each company should consider the implications of applying such terminology, as inaccuracies may result in crisis events being ignored, or conversely, common issues resulting in disproportionate levels of management attention and resource allocation. Common sense and experience will play a key role in guiding managers; however, some simple tools and definitions will support a common understanding across an organization. Such definitions might include:

- **Problem.** An everyday occurrence that does not affect an individual's safety, the integrity of critical infrastructure, or the protection of sensitive materials or information, and does not undermine significantly the operational productivity of a project, nor devalue the business interests or reputation of the company.
- **Crisis.** A singular event that places employees at personal risk (whether physical or psychological), threatens the integrity of critical infrastructure, may lead to the loss of sensitive materials or information, hinders the operational productivity of a project, and presents a threat to the business interests and reputation of the company.

Many large corporations have grown through mergers with or acquisitions of other organizations, or operate within the market space through joint ventures and teaming agreements. In these cases, there is a rapid assimilation of multiple organizations' approaches to risk management, which adds a significant degree of complexity to definition and subsequent management of risk. Aligning different approaches, requirements, and expectations is critical to ensuring that complex and integrated organizations can best manage a crisis event.

Mapping Risks

Mapping risks should occur as a layered approach to enterprise resilience. It should be a top-down driven approach, meeting strategic, operational, and tactical risks in a logical and pragmatic manner. Enterprise resilience should consider the following key questions when designing the strategy:

- What is the company's risk tolerance? How can perceptions be formalized?
- How can risks be measured, tracked, and monitored? Who is responsible and how do they do this?
- What are the company's key earnings? What market and financial risks are there?
- Where does the company operate? What environmental risks are there?
- What is the company's cultural approach to risk? What are the ethos drivers?
- What liability and reputational risks are there? What impacts could result?
- Are there pan-corporate risks? What are the pockets of singular risks?
- How effectively are traditional and strategic risks being managed? Is there any supporting information?
- What knowledge, experience, and capability does the company have? Where are the gaps?

Companies can then develop a framework for designing a risk management architecture in order to manage both the tangible and nebulous risks facing their corporation and business activities. During the design of the Business Continuity Management Plan, companies should consider:

- What capabilities are available in-house, and which must be outsourced?
- What information does the board require to manage risks, and what can be delegated?
- How are risk management groups to be structured, and what interfaces are required?
- How can threats be mitigated? What impacts could result if a risk event occurs?
- How will communications be channeled? What authorities and permissions will be sanctioned?
- How will policies, plans, and systems be managed? Who takes the lead?
- How will quality assurance and monitoring be conducted? What are the metrics?
- How are supporting agencies managed? What agreements are in place?

During the implementation of a resulting risk management system, companies should ensure that the approach is supported at all levels and keep current with the fluid risk environment. Implementers of corporate risk management should consider:

- How does the corporate board ensure that it has the information it needs? How does it monitor the group's performance?
- What sensing mechanisms are in place? How are risks identified and forecast?
- How are risks measured and tracked? What metrics trigger a response?
- How can policies, plans, and systems be kept current? What investments or resources are required?

- How does the corporate culture support and sustain the risk management approach?
- How are policies shared and empowered? What training is required?
- How does information technology and other resources support implementation? What infrastructures are required?
- What are the cost benefits to risk management? How much capital investment and indirect costs should be apportioned?

The development of a strategic risk management approach will support individual business efforts across widespread operating theaters. By establishing a strategic appreciation for risk, companies can then better support singular project activities through a unified and mature and appropriately organized approach.

Critical Dependencies

The Business Continuity Management Plan should map out the critical dependencies that will affect the company's ability to operate under crisis conditions. Critical dependencies may also affect the safety and security of personnel—and might include the supply chain assurance of critical materials or services; the ability of the company, its vendors, partners, and clients to undertake or receive services; or any effects an emergency might have on the company's personnel.

The following areas of critical dependency are offered as sample considerations when designing a Business Continuity Management Plan:

- **Power and Utilities.** The reliance and risk exposures that might result from the disruption to power and other utilities on which the company, its activities, or personnel might be dependent.
- **Supply Chain Assurance.** The risk exposure and business disruptions that might occur if critical materials and supplies are delayed, damaged, or stolen—in terms of safety and security as well as business performance.
- **Critical Materials or Structures.** The risks that might be present if critical structures, facilities, or materials are lost, damaged, or stolen—in terms of performance, liability, and physical risk natures.
- **Employee Confidence.** The implications of a loss in employee or workforce confidence should they be exposed to risks that undermine their ability or willingness to work.
- **Vendor or Teammate Performance.** The degree of dependence a company has upon vendors or teammates should they be affected by risks or disruptions that might not directly affect the company.
- **Governance.** The importance of governance and social stabilities within an operating region as a holistic component of operational success and risk and security management.
- **Technology and Information.** The risk implications and impacts should technologies be damaged, corrupted, lost, or stolen either from the company or from its clients or vendors.

The examples provided are in no means exhaustive and demonstrate only some of the generic dependencies that can curb, disrupt, or stop safe and effective business operations—either directly or as a secondary effect resulting from a crisis.

Tactical Risk Evaluations

The Business Continuity Management Plan should also seek to map the common traditional risks faced by the company within different operating environments. Risks are fluid and can change rapidly due to unforeseen circumstances. However, by structuring a risk evaluation framework, the company can better place its business interests and operations into an understandable context. Risk evaluations are complex and subjective assessments, and clear and consistent matrixes for evaluating impact and probabilities are required.

By conducting such evaluations, companies can more clearly identify where their greatest risks may lie, as well as where finite resources should be focused in order to mitigate postulated threats to personnel, facilities, operations, and business interests. Risk evaluations can be conducted at a strategic level to gain a macro perspective of where challenges may lie, but should also be conducted at a local perspective, as the risk landscape within a country may differ significantly from region to region, from city to city, and in some instances from neighborhood to neighborhood. The company may also wish to consider the following points when mapping and assessing risks:

- **Hard and Soft Targets.** Is the company an easy target compared to similar businesses or operations within the region, or are hostile groups more likely to achieve success focusing on less protected companies?
- **Common or Unique.** Are certain risks common within a particular environment, or would they be considered unique or unusual if they were to occur?
- **Incentives and Objectives.** What are the incentives and objectives of hostile individuals or groups? What are they trying to achieve, and how might they best achieve their goals?
- **Capabilities and Trends.** What are the realistic capabilities of hostile groups—do they have the knowledge, technology, and funding to be successful, or are they unable to launch sophisticated attacks? Do any trends support this analysis, or suggest future risks?
- **Mitigation Reliability.** What mitigation measures have been created to deal with risks against the company or its personnel? What gaps remain, and how effective are the measures? Should gaps then be addressed, or only acknowledged?
- **Impact Evaluations.** What impacts will be associated with an incident, both to the company and its personnel, as well as to surrounding areas and populace? Consider the holistic impacts and ramifications of each risk type. Also, how does this impact teammates and subcontractors?
- **Tolerances.** What tolerances does the company have, as well as the pertinent government, population, and legal systems? How much risk will be accepted by each group, and where do tolerance-level risks get breached?
- **Response Capacity.** What response measures and capabilities are available to deal with a crisis? Do government or supporting bodies have the knowledge, resources and interest in assisting the company, or will they part of the problem? What outsourced and in-house capacities are available and might be brought to bear?

Exhibit 1.2, Strategic and Regional Risk Mapping, illustrates a simple method by which to gain a strategic picture of risk probabilities for a range of countries in

	Albania	Algeria	Afghanistan	Bulgaria	Belarus	Chili	Egypt	Iraq	Kuwait	Libya	Pakistan	Thailand
Strategic Risks												
• Opportunistic Crime	5	4	3	2	1	3	4	3	2	2	3	4
• Organized Crime	5	4	3	3	1	2	3	3	1	1	3	3
• Insurgency and Terrorism	2	3	5	1	1	3	2	5	1	2	3	1
• Social Infrastructures	3	3	3	3	2	2	2	3	1	3	2	2
• Political Stability	3	3	3	1	1	2	2	3	1	2	2	3
Specific Man-Made Risk Types												
• Kidnap and Ransom	3	4	3	1	1	2	2	3	1	1	3	1
• Domestic Terrorism (Special Interest Groups)	1	1	1	1	1	1	1	1	1	1	1	2
• Blackouts	4	3	4	2	1	1	2	3	1	1	4	1
• Road Traffic Accidents	4	4	3	2	2	1	4	3	2	3	4	2
• Mugging and Robbery	4	3	2	2	1	1	4	3	1	2	3	2
• Arrest and Detention	3	2	1	1	1	1	2	1	1	2	2	1
• Unexploded Ordnance and Mines	3	3	4	1	1	2	1	2	1	1	2	1
• Indirect Fire Attacks and Small Arms Fire	1	1	3	1	1	1	2	3	1	1	2	1
• Threats, Coercion, and Intimidation	5	4	3	2	1	2	3	2	1	2	3	1
• Nuclear, Biological, Chemical Attacks	3	2	1	1	1	1	2	3	1	1	3	1
• Complex Attacks	1	1	4	1	1	1	2	4	1	2	4	1
• Explosive Attacks and Sabotage	2	3	5	1	1	1	2	5	1	1	3	1
• Fraud and Corruption	5	4	5	3	2	1	4	4	1	2	3	1
• Espionage and Counterfeiting	5	3	2	2	1	2	3	2	2	3	4	2
• Demonstrations or Civil Disturbances	2	2	3	1	1	2	3	4	1	1	4	1
Specific Natural Risk Types												
• Floods	2	1	2	1	1	2	1	1	1	2	3	3
• Earthquakes	2	1	1	1	1	2	2	1	1	2	4	3
• Pandemics	2	3	4	2	1	2	4	3	2	2	3	4
• Tidal Waves	1	1	1	1	1	2	2	1	1	3	1	4
• Hurricanes and Tornadoes	1	1	1	1	1	2	1	1	1	1	2	3
• Volcanoes	1	1	1	1	1	1	1	1	1	1	2	1
• Sandstorms	1	3	1	1	1	1	3	4	4	3	1	1
• Landslides	3	3	3	2	3	3	3	2	2	2	2	2
• Forest Fires	2	3	3	2	2	2	1	1	1	2	2	3
Risk Grading Table	**H**	**M**	**L**	**H**	**H**	**L**	**M**	**N**	**H**	**L**	**M**	**N**
1 Negligible Level of Risk—Highly Unlikely to Occur	**Company Footprint**											
2 Low Level of Risk—Remote Chance of Occurrence	**H** High—50-plus full-time expatriates and 100 locals											
3 Medium Level of Risk—Some Chance of Occurrence	**M** Medium—30–49 full-time expatriates and 50–99 locals											
4 High Level of Risk—Likely to Occur	**L** Low—10–29 full-time expatriates and 20–49 locals											
5 Extreme Level of Risk—Expected to Occur	**N** Negligible—1–9 full-time expatriates and 1–19 locals											

EXHIBIT 1.2 Strategic and Regional Risk Mapping

which the company may be operating (note that the numbers are not evidenced evaluations, and changing conditions will alter such gradings). Such simple tools, however, are relatively easy to maintain and provide a mechanism for guiding management decision making and resource allocation as they can represent risks within a visual or comparative manner. Risk mapping systems also allow for a consistent approach to be replicated throughout an organization so that a consistent evaluating tool is available to all levels of managers.

Risk evaluations should be supported by current intelligence and threat evaluations and should be kept live. Local assessments should feed into a strategic risk evaluation table to ensure consistency of risk calculations. Such tables should guide managers in terms of devoting time, resources, and effort to developing specific components of the Business Continuity Management Plan such as pandemic response policies, evacuation plans, contracting response agencies, and security professionals. In addition, such grading also illustrates where finite resources and investment should be focused, rather than waste time and effort on areas that might have less risk than others.

Determining Risk Tolerances

Defining risk tolerances within a company can be problematic, as perceptions and opinions vary significantly. There may also be a reluctance to document certain policies due to liability concerns. That said, where possible the company should attempt to define clinically what constitutes a low, medium, high, and extreme risk or threat level in order to avoid ambiguity. Exhibit 1.3 is an example of a simple risk tolerance table that illustrates how a company might capture tolerance levels for the group or for an individual project.

This simplified approach also ensures a consistent approach within a company, although regional and project differences should be applied since what constitutes a low threat for one region or activity may be considered a high threat for another. Risk tolerance tables should also be connected to alert states and trigger response plans (where appropriate) to ensure that response measures reflect risk tolerance levels.

Incident Response versus Crisis Management

The effective management of a crisis situation will be conducted by a number of response groups, each undertaking unique tasks, but with many overlapping functions. Some of the response groups may have no training or experience in dealing with a crisis situation. Others may have considerable experience and knowledge, supported by well-established policies and procedures, with well-resourced and practiced support structures. Typically for most companies, the first line of defense against an emergency situation consists of nonsecurity specialists: the receptionist, office supervisor, or work site manager. In addition, response groups are often built around need, with the mobilization of both internal and external resources to meet new and unique challenges as they occur. For the purposes of simplicity, three groups are typically required within a crisis management situation:

1. **Immediate Response Group.** The nonspecialists who by chance happen to be the first persons at the center or point of the problem and who initiate the predefined incident and crisis response groups while feeding information upward to support decision making. These individuals may also start dealing with the crisis requirements. Often the immediate response group will be subject to, or be victims of, the emergency situation itself.
2. **Incident Response Team.** A predefined or event-mobilized team whose responsibilities are to deal solely with the specific event in hand—the micro crisis—focusing mainly on the security and safety aspects associated with the

EXHIBIT 1.3 Simple Risk Tolerance Table

Risk Nature	Low Threat	Medium Threat	High Threat	Extreme Threat
• **Civil Unrest**	Nonviolent group of 5–15 persons	Semiaggressive group of 5–15 persons	Aggressive group of 3–15 persons	Aggressive group of more than 16 persons
• **Missing Person**	Has not been sighted for more than 6 hours	Has not been sighted for more than 12 hours	Has not been sighted for more than 24 hours	Has not been sighted for more than 72 hours
• **Fatality**	A single natural death over the course of one year	More than three natural deaths over the course of one year	A single death due to hostile actions over one year	More than two deaths due to hostile actions over one year
• **Theft**	The theft of nonvaluable items from a project	The theft of semivaluable items from a project	The theft of valuable items from a project	The theft of critical items from a project
• **Vehicle-Borne IED**	An explosion within another city in-country	An explosion within a remote part of the city	An explosion within an adjoining neighborhood	An explosion in the immediate vicinity
• **Hurricane**	A hurricane within the country or state	A hurricane within the state or county	A hurricane within the county or area	A hurricane within the immediate vicinity
• **Flood**	Minor flooding within the state or region	Major flooding within the state or region	Major flooding within the immediate area	Flooding that directly affects the project
• **Complex Attack**	Complex attacks conducted in-country	Complex attacks conducted in the region	Complex attacks against a similar organization	Complex attacks targeting the project or company
• **Evacuation**	Risk environment requires an evacuation alert	Risk environment requires no essential work to stop	Nonessential project personnel evacuated	Essential project personnel evacuated
Caveat	*Common sense applies when assessing the risks posed to personnel, operations, facilities, and materials. These are provided as guidelines only to remove unnecessary ambiguity and provide managers a framework from which to operate.*			

event. They will have tactical decision-making authority to manage the actual event and will take strategic direction from the crisis management team.

3. **Crisis Management Team.** A predefined team whose responsibility is to coordinate the activities of the incident response team in alignment with external agencies and groups, as well as managing the macro-level impacts and effects beyond the actual incident itself. Often this team is specialist in nature and remains on task after event closure, as well as after the incident response team has stood down, to conduct postincident reviews and evaluations.

Where possible and appropriate, management responsibilities should be delegated to the lowest levels, as these are the points at which most crisis or incident management occurs. The coordinated and combined activities of all three groups are designed to ensure that a company is in a position to effectively respond to postulated or occurring threats in a timely, coordinated, and effective manner. Top-level management commitment and sensible and usable policies and plans are critical for the success of the crisis response policies and procedures.

Stages of Incident Management and Crisis Response

There may be numerous steps within a crisis event sequence (see Chapter 2), and the Business Continuity Management Plan should take these into consideration, determining what policies and plans are required for each stage, as well as how best to transition between different management stages. The IMP could be considered the method by which to deal with the immediate response stage, allowing for the effective transition to the interim and follow-on response stages. The immediate response stage should be focused on preventing the threat from growing, saving lives and property, and feeding information to defined incident management and crisis response teams, as illustrated in Exhibit 1.4.

Understanding Risk

The concept of risk is complex, subjective, and often fluid. Often a threat will be perceived differently by various individuals, organizations, and groups. Company and individual tolerance levels also play a part in the assessment of risk, as some companies have low tolerance levels, while others are more robust in their acceptance—and this also frequently shifts over time, or is driven by events. Risk

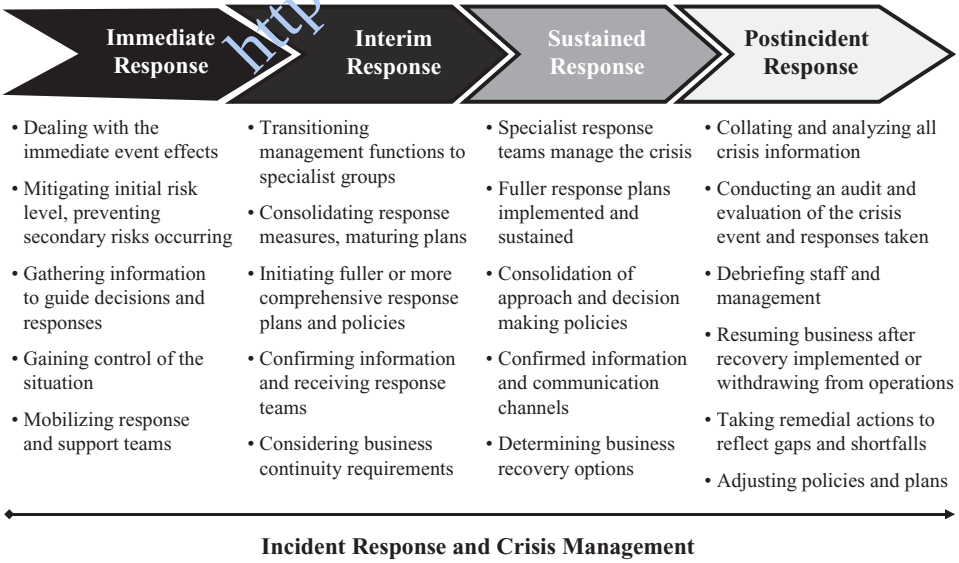

EXHIBIT 1.4 Stages of Incident Management and Crisis Response

is effectively a phenomenon that either directly or indirectly affects businesses and employees in terms of productivity and safety. For practical purposes, risks can effectively be categorized into:

- **Personnel Risk.** It is important that companies apply due diligence to the screening and selection of their employees through reliable background investigations. This is especially important for management roles or those positions with access to sensitive information.
- **Competitive Risk.** Business activities are at risk if companies are not cognizant of how competition is strategizing commercial activities, placing them at a commercial disadvantage. Investigative services and analysis can provide companies with advice and guidance on how to compete in their markets.
- **Due Diligence Risk.** A company must be confident that its client, partner, or subcontractor is appropriate in terms of closing deals involving legal, liability, or capital investments. Investigative services can ensure that companies are reputable and appropriate to engage with.
- **Reputation Risk.** Brands and reputations underpin the status and reliability image of a business; therefore, damage to either brands or a company's reputation can undermine its commercial productivity.
- **Information Risk.** Information technology (IT) enhances commercial productivity; however, it also leaves companies vulnerable to data theft or loss. Industrial, criminal, government, or terrorist espionage has serious implications for businesses, and IT must be physically and technologically protected.
- **Intellectual Property Risk.** Commercial espionage or organized crime poses a serious threat to established products as well as emerging markets. Intellectual property is subject to theft or replication, which would undermine the value of the producer's performance.
- **Physical Risk.** Crime, insurgency, terrorism, civil unrest, and natural disasters are unpredictable and have significant impacts on companies and individuals. Risk mitigation, contingency planning, and crisis planning can be used to offset the spectrum of risks facing a company.
- **Political Risk.** Political instabilities have considerable impacts on global companies, as well as those operating within their parent country. The analysis and assessment of opaque and uncertain political environments will aid clients in complex political environments.

Risks can also be considered in terms of *internal risks* (those risks resulting from employees or company activities directly); *supported internal risks* (those risks resulting from external groups, supported by employees); or *external risks* (those risks that are a result of purely external action or attention). The concept of a risk, or indeed a crisis, is also influenced by varied and complex factors that will shape how an organization plans for and manages a wide spectrum of threats to its operations, including:

- **Subjectivity.** Risk is open to different interpretations, which themselves often change.
- **Perceptions.** Risks are influenced by human experience and opinion.
- **Tolerances.** Risks are determined by personal or group risk appetites.

- **Understanding.** Knowing what risks are and their impacts defines how organizations approach risks.
- **Fluidity.** Risks often change quickly and with little warning, rarely remaining constant.
- **Mapping.** Mapping risks presents challenges, as risks can cause unpredictable effects.
- **Quantification.** Risks are often difficult to clinically prove or gauge until after the event.
- **Measurability.** No infallible methods by which to measure risk impacts or probabilities.
- **Unpredictability.** Risks are unpredictable and may cause varied effects and follow unpredictable paths.
- **Diversity.** Risks are often numerous in number and nature.
- **Complexity.** Risk are often interrelated and with multifaceted considerations.

TIME, SPACE, AND IMPACT Risk can also be considered in terms of *time*, *space*, and *impact*. Some risk events are shortlived, while some are prolonged. Risks may be defined within a specific geographic or corporate interest area or space, whereas others may span a wide geographical and corporate interest area. The impact of a risk may be either minimal or far-reaching, as illustrated in Exhibit 1.5, Risk: Time, Space, and Impact, which demonstrates how a risk might have a medium impact and life span but impact a large area of interest or space. The Business Continuity Management Plan and its various components should include these three aspects of risk when considering appropriate contingency planning and crisis response measures. While a conceptual rather than a practical tool, such concepts help focus those developing or implementing contingency planning or crisis response measures in defining the nature, scope, and life span of possible risk events, and thus assist them in placing those events into some form of context to aid planning and impact visualization. Companies may choose to use such models for each risk type within a corporate context, or as a risk relates to a specific project or business activity.

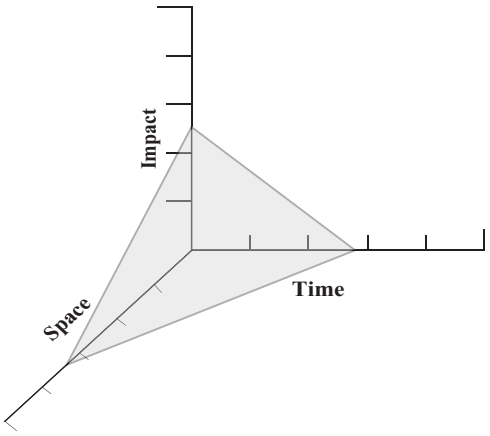

EXHIBIT 1.5 Risk: Time, Space, and Impact

PROBABILITY Risks also come in varied levels of probability, ranging from low, where the probability of a risk occurring is highly unlikely, to extreme, where the company should expect a risk to occur at some stage. By clearly defining category levels, the company will quickly come to understand the evaluated probability of risks occurring to its business activity. The IMP should also be attuned to these risk and probability levels, as the operational decisions made by company management utilizing the incident response guides will be aligned by risk perception and the associated impact and probability levels. Some examples of how a company may attach risk management activities against risk levels are provided as a basic guideline:

- **Low Risk.** The probability of a risk occurring is unlikely, and no special or costly measures should be implemented other than standard company policies and procedures—unless the risk nature has a significant impact on the company. A detailed Business Continuity Management Plan may not be necessary, and risk awareness training may be useful only on an annual basis. The use of only a simple IMP may be appropriate.
- **Medium Risk.** The probability of a risk occurring is possible, and risk mitigation measures should be reflective of the costs and impacts of the risk on the company and the business activities, captured within a basic Business Continuity Management Plan. Low-level management training will be beneficial to the company and project groups on an annual or semiannual basis. A more focused IMP should be developed.
- **High Risk.** The probability of a risk occurring is likely; therefore, the company is advised to establish an appropriate budget to set up policies and procedures to counteract the probability of the risk occurring, as well as the subsequent impacts within a detailed Business Continuity Management Plan. Thorough management training on a semiannual or regular basis will support the organization in responding to any crisis event more effectively. A mature IMP should be in place and tested periodically.
- **Extreme Risk.** The risk is certain to occur at some stage of the project activity's life span. Therefore, the company should be advised to consider whether to continue with its activity, or acknowledge the impacts and responses within a detailed and tailored Business Continuity Management Plan, with frequent and detailed desktop exercises for varied levels of the management structure. The IMP should be connected to external organizations and agencies, and be tested and evaluated on a scheduled basis.

Often company risk tolerances are fluid and levels of risk acceptance will adjust to changing business needs or leadership perspectives. Companies also become desensitized to a risk over time, and what might have been considered a significant issue gradually becomes the norm over time or repeated exposure to a particular crisis event. Conversely, a catastrophic event outside of a specific project location might sensitize a company to risks faced in other activities, regardless of proximity or project similarity. Corporate and local risk appreciation and tolerances also frequently differ. Those project managers living the risk might disagree with their corporate counterparts on how serious a risk might be, and how best to mitigate the

threats. Often this will lead to a conflict into which a vendor company or middle managers within a company might be drawn. Also, this will affect how field and corporate officers approach risks. Those responsible for risk and security management must be aware of these dynamics and should seek to represent risks using factual and clinical information where possible, with an appreciation of the dynamic tolerance and perception influences at play within the organization. The IMP is a tool used to address a risk when warning indicators are triggered or when an emergency is occurring, and as such must at all times reflect the company's official perceptions and policies.

Immediate Response and Impact Levels

The nature of the crisis event will determine the intensity, tempo, and range of effects that occur in the immediate term, near term, and long term. Some crisis events will see peaks and troughs of business or operational impacts over a protracted period. Others will see a surge of risk at the front of the event, with declining effects over time. What is true of many crisis events, however, is that the greatest degree of impact occurs at the beginning of a crisis event. This is also the period that provides the most potential for a well-prepared company to gain control over a situation, or indeed the period at which the worst effects are felt as the greatest confusion and most errors occur within an organization.

Exhibit 1.6, Immediate Response to Impact Levels, illustrates that as a general rule the greatest impact of a crisis occurs at the outset of an event, whether this is

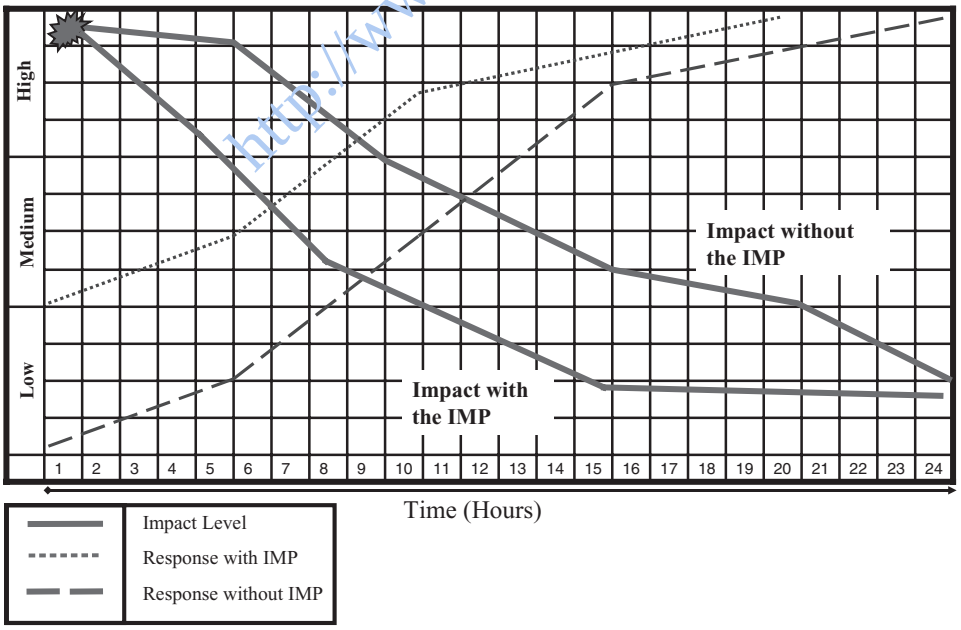

EXHIBIT 1.6 Immediate Response to Impact Levels

a forest fire, an earthquake, a hostage situation, an aircraft crash, or an industrial accident. Typically, over time the effects of the event decline as either the cause diminishes in intensity or is no longer present, the situation stabilizes itself, the initial confusion and panic decline, government or company resources are committed to respond to the problem, or appropriate company managers assume responsibility and address the threat. As shown on the graph, the level of preparedness defines how quickly control is brought to a situation, as well as the possible impact levels associated with a crisis event. The graph illustrates a subjective representation of how impact levels correspond to the ability for an organization to bring swift and effective control to a crisis; the impacts being brought under swift control with effective response measures in place, while impact levels continue at higher levels if response measures are not in place.

As the greatest level of confusion and impact generally occurs within the initial minutes or hours of a crisis event, it makes sense that an appropriate amount of focus be applied to supporting expedient and effective management responses for this stage within the crisis. A company that provides pragmatic guidance and tools to the first responders or local incident managers will generally gain better control over the event, more accurately grasp the scope and nature of the situation, and as a result develop better management approaches and decisions at the outset of a crisis in order to exert the most effective controls. In addition, supporting the local incident managers assists more experienced crisis managers in understanding the problem and responding through knowledge driven responses. Invaluable time is frequently lost during the most critical stages of a crisis situation as managers attempt, often with little success, to understand what is happening, make appropriate decisions, and mobilize essential resources to deal with the issue.

Risk Management

It is important both within the company, but especially within supporting vendors and agencies, that the different levels of focus and need within a crisis event are understood in order to develop and implement an effective Business Continuity Management Plan and associated elements such as the IMP. Corporate officers will require support in terms of strategic planning and business resilience and recovery requirements, while project managers will be dealing with more front-end-related operational issues such as resolving immediate and granular level threats to their personnel, materials, or project activities. Many focuses and needs will overlap, where both groups will be striving to reach the same overall goals; however, the particular focus areas associated with each group will determine what information or participation is needed, what parameters of authority and decision making are permitted, as well as what systems and tools will be most required. It will also shape how an organization might reach outside of its own capabilities and knowledge to tap into government or commercial groups for support. It is especially important that security and other supporting vendors understand the different needs and expectations of the different layers and groups within a company in order to provide more effective support. The Chief Security Officer of a company should also be thinking along this lines of requirement in order to direct internal and external resources. The security vendor should think in terms of corporate, country, and

project issues, with the field security managers dealing with the immediate tactical requirements of incident management as part of the larger crisis approach. The country and corporate security vendor managers assist with providing strategic guidance and support, as well as assisting with the transition from immediate incident management to interim and sustainable crisis management and recovery measures.

Contingency planning presents an opportunity for the company to reduce the level of risk to its corporate structure and business activities, as well as establish a plan by which to deal with problems, while not under the pressures of the crisis event itself. It is often a failing of organizations not to develop an appropriate risk management approach, paying lip service to the creation of a pragmatic and current Business Continuity Management Plan (in which the IMP belongs), which often results in serious mismanagement and confusion during an emergency. Those organizations that engage effectively in contingency planning can significantly reduce the problems resulting from a crisis by responding in a more organized and focused manner, considerably reducing both the initial and long-term effects and impacts of a crisis, while concurrently supporting overall business continuity and recovery.

Incident management is the first step of a broader crisis management approach, often involving local project managers who will play instrumental roles in collecting vital information relating to the event, which then determines both decision making and response actions. Often incident management is the response to a problem while it is occurring, or immediately following an incident. Crisis management itself may continue long past the event and involves the broader (rather than tactical) considerations associated with an emergency, as the lingering effects of the incident persist. Incident management planning addresses the threats posed should risk mitigation measures (risk mitigation and security response plans) not be successful or should the security or risk management measures be breached. These management plans are methods by which to reduce potential business impacts or losses, and they should be readied for the company's incident response and crisis management teams to implement. There are effectively three forms of crisis that leadership might face within a company:

1. **Strategic Crisis.** A change in the business environment might call the viability of the company or activity into question (e.g., loss of productivity, hindrances to operations, serious equipment losses, or injuries or deaths that undermine commercial ventures).
2. **Public Relations Crisis.** This is more commonly called *crisis communications* (e.g., negative publicity that could adversely affect the success of the company, media coverage of liability claims, reputational damage, employee morale issues, and publicized government and legal investigations that can affect stock shares and company confidence).
3. **Financial Crisis.** These crises are typically short-term liquidity or cash flow problems and long-term bankruptcy problems. Financial crises can often result from strategic and public relations crises.

Typically, the IMP focuses on the strategic crisis, although it touches upon and influences public relations and financial crisis factors as risk events are often

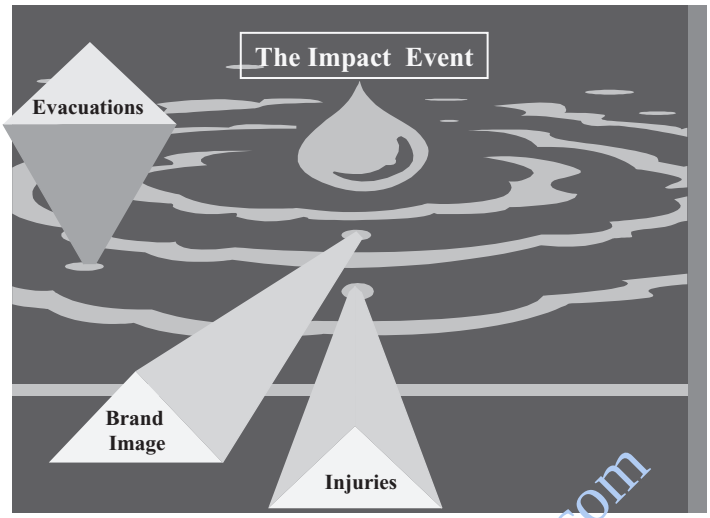

EXHIBIT 1.7 Risk Ripple Effects

interrelated and result in ripple effects that move through different areas of risk (as illustrated in Exhibit 1.7), where a singular event can create secondary hazards to a company.

The IMP addresses the immediate and tactical aspects of the crisis prior to more comprehensive and sustainable crisis responses being implemented. Established management structures, communication plans, decision matrixes, and trigger response plans should be designed to ensure that responsibilities are attributed and communication channels understood to support the overall Business Continuity Management Plan (see Chapter 2).

Response Trigger Points

Defining when a problem becomes a crisis is important, as perspective may play an important part in defining when a crisis is actually occurring. The IMP may be used both to avoid a problem developing into a crisis and in dealing with the first stages of a crisis event itself. For example, the need to evacuate a nuclear reactor facility may occur when several risk levels have been breached: Insufficient electricity is being provided to power a water pump, the reactor water-cooling system fails, the redundancy systems fail, and a reactor reaches a critical temperature. The Business Continuity Management Plan should define *trigger points* that identify when a problem has become a crisis, and at what level the crisis situation is rated. Trigger points can also be used to avoid a crisis by identifying an approaching problem so that measures can be implemented by which to avoid the effects; for example, elections are imminent in a volatile region—evacuation plans are reviewed; public disturbances start occurring—nonessential staff withdraw; government forces use unnecessary force—remaining personnel move to a safe location; mass riots occur—the company has already withdrawn from the risk area.

Companies should establish defined events or factors that require a predetermined action or activity—the trigger. Trigger points are connected to the decision matrix and will be the catalyst for decisions; for example, increased local tensions may result in a scaled response from the project leading to only critical external work being conducted and subsequently to the measured evacuation of the site itself. Trigger points may be aimed at various levels; the injury of a project employee by hostile action may require the executive board to review whether it wishes to remain on task and whether increased security measures are required. Rising community tensions may cause a local manager to stop operations and send staff home. Thus trigger points and decision matrixes may be engineered at three levels: corporate, country, and project. However, all levels should overlap, because a corporate decision or trigger will have repercussions on country and program activities and policies, and local decisions or triggers may result in corporate concerns and activities.

The grading of trigger points is subjective, driven by project staff and company tolerance perspectives. However, where possible a definitive statement should be attached to a risk-level description as well as the nature of the threat. Thus a low threat might be graded as a 2, and the definition might include: *The probability of likelihood is considered low to remote, with resulting impacts also rated low.* Some risk factors might have a low probability, but a high impact (a shooting, bomb, or tsunami) and so a definition might include: *The probability of likelihood is considered low to remote; however, the resulting impacts are rated as catastrophic.* The grading on a trigger response table may need to be more fully explained than purely attributing a numerical value.

Often companies that define triggers do not enact them, having a tendency to delay a decision in order to see how an event may unfold as a decision might affect operations, reduce performance or call into question the decision maker's judgment. Delaying the implementation of a trigger response can devalue the Business Continuity Management Plan and prevent effective crisis avoidance and management from occurring. Exhibit 1.8 shows where managers may delay a trigger, and the possible resulting implications.

EXHIBIT 1.8 Failure to Follow Trigger Points

Trigger	Action	Delayed	Impacts
Flood Warnings	Evacuate area and sandbag facilities.	Managers wait for floods to actually start occurring.	Personnel are stranded as roads are closed, and property is damaged as not protected.
Hurricane Warnings	Move to alternative work areas and batten down facilities.	Managers wait for hurricane's direction to be confirmed.	Personnel are exposed to avoidable risks and property is damaged as not protected.
Bomb Threat	Evacuate buildings and search for suspicious items.	Managers wait until law enforcement advice or support arrives.	Explosion occurs, injuring occupants and exposing company to liability claims.

Managers should be advised it is better to "pull the trigger" than delay making decisions or alerting crisis managers. As such it is often better to pull the trigger (as defined in advance through contingency planning) as a safety measure, rather than resorting to a decision delay approach, and thus move past a predefined response protocol. Although a measured, mature, and well-informed decision is always preferable, inaction due to uncertainty or a lack of management confidence exposes the company and its personnel to avoidable risk.

Exhibit 1.9 illustrates a simple trigger response matrix that allows various elements of a crisis response organization to understand at what point a certain trigger response is required. As much subjectivity as possible should be removed from such a grading approach; there should be a focused and unambiguous description of what each crisis event and response means and entails.

Crisis Event	Threats, Coercion, and Intimidation of Local Nationals	Rising Incidents of Violence toward Local Employees	Rising Levels of Violence toward Expatriates	Reduced Rule of Law and Increasing Public Tensions	Increasing Civil Gatherings and Disturbances	Widespread Riots and Loss of Rule of Law	Possible Intelligence—Targeting of the Company	Possible Targeting of Co-Located or Adjacent Groups	Specific Intelligence—Targeting of the Company	Specific Targeting of Co-Located or Adjacent Groups	Increased Levels of Road Blocks or Illegal Vehicle Stops	Aggressive Tactics by Police and Host Nation Military	Arrests and Detentions by Local Government Forces	Arrests and Detentions by Local Militia	Western Embassy Threat Warnings and Alert States	Increasing Number of Unarmed Attacks on Personnel	Increasing Number of Armed Attacks on Personnel	Increasing Number of Unarmed Attacks on Facilities	Increasing Number of Armed Attacks on Facilities	Specific Targeting of Supply Chain	Targeting of Project Staff Moving to Project Locations	Targeting of Western Companies within Operating Area	Targeting of Local Subcontractor Companies
Increase Alert Status	2	2	2	1	1	1	2	3	1	2	2	2	1	1	2	3	2	3	2	3	2	2	3
Increase Risk Posture	2	3	2	3	2	3	2	3	2	3	3	3	3	2	3	3	3	3	3	4	3	3	4
Noncritical Travel Stops	3	3	4	4	3	3	3	4	3	4	3	4	4	3	4	3	4	4	4	5	4	4	5
Critical Travel Stops	5	4	5	5	3	4	5	5	4	5	5	5	4	4	5	5	4	4	4	5	4	5	5
Facility Security Posture Increases	4	4	4	3	3	3	3	4	3	4	5	4	4	4	4	5	4	4	3	5	5	4	4
External Project Operations Stopped	4	5	4	4	3	3	4	5	4	5	4	4	5	4	5	5	4	5	4	5	4	5	4
Project Facility Closed Down	5	4	4	4	3	3	5	5	5	5	5	5	5	5	5	5	4	5	4	5	5	4	5
Local Employees Stood Down	4	3	5	4	3	3	5	5	5	5	4	4	4	3	5	4	3	5	4	5	5	4	4
Stage 1 Evacuation	4	4	4	4	4	3	5	5	4	5	5	5	5	5	5	5	4	5	4	5	5	5	5
Stage 2 Evacuation	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5

Level	Trigger Response Guide
1	Negligible levels of risk with low-impact threats to the project, personnel, or resources
2	Limited levels of risk with low to some impact threats to the project, personnel, and resources
3	Medium levels of risk with noticeable impact threats to the project, personnel, and resources
4	High levels of risk with significant impact threats to the project, personnel, and resources
5	Extreme levels of risk with unacceptable levels of impact threats to the project, personnel, and resources

EXHIBIT 1.9 Crisis Management: Trigger Response Matrix

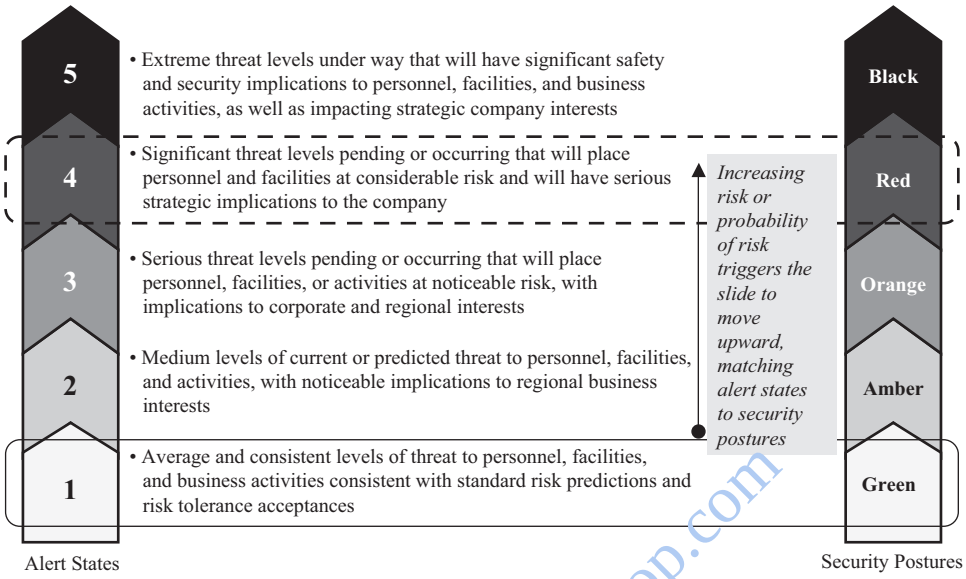

EXHIBIT 1.10 Crisis Management: Simple Trigger Response Tools

Companies can also utilize more simplistic and targeted trigger tools in order to allow managers to move through response levels in a systematic and logical manner. This may be related to a specific activity or function, such as facility security responses to triggers, movement configurations and profiles, international travel permissions, or any other aspect of the company's business that might change to reflect shifting risk levels. Exhibit 1.10, Crisis Management: Simple Trigger Response Tools, illustrates how certain risk levels, or the probability of risk increases, might be used as a sliding scale to prompt changes within an emergency alert state. These alert states in turn may be connected with movement security levels, with tier 1 personal security details at alert state 1 being amalgamated or augmented to provide increasingly more robust security configurations to reflect the threats posed to traveling project staff as the threats move upwards to alert state 4. Such sliding scales can be used for facility security postures or other simple response levels, removing much of the ambiguity of decision making, while also evidencing for postincident reviews and other audit requirements the rationale and processes used to safeguard personnel and other company interests. The company security plan for a facility can be linked to such tools, connecting alert states to ranging security postures and protocols.

Such tools can be used to define numerous security management procedures and responses which are triggered by intelligence or certain risk tolerances being breached.

Decision and Authority Matrixes

Every element of the Business Continuity Management Plan, whether it is the corporate policies and management systems or individual crisis and management policies

and plans such as the IMP, should be developed in alignment with defined decision matrixes and management authorities to ensure that action responses and information chains are best managed within an organization or group. Decision matrixes enable effective decision making by those best placed to determine and implement the required courses of action to bring control to a crisis event (see Chapter 2). Company management should not be debating which employee has decision-making authority, or the parameters of their permissions, while an emergency is under way, as this impedes clear and effective management at the most critical stages of an event and distracts an organization from effectively responding to an emergency. As a crisis escalates, the decision-making authorities may ascend upward to the executive board, and the point where the impacts breach certain authorities should also be clearly defined. Therefore, the Business Continuity Management Plan should clearly define authorities for decisions associated with postulated activities or responses in order to reduce as much organizational confusion as possible during a crisis event. By having decision areas and authorities defined prior to an event occurring, management can also be provided training and guidance on their lines and areas of authority, as well as be empowered to take decisive action where necessary and appropriate. Gaps and shortfalls within risk management policies and plans can also be better identified, as ownership of response and accountability of action are more clearly defined within the company. Exhibit 1.11 illustrates a simple decision and authority matrix that defines which management groups are sanctioned to implement specific policies and plans.

Each area should have a subset of instructions that unambiguously define what each response means. The instructions may be complex and detailed, such as evacuation plans, or simple and succinct, such as the destruction of sensitive materials. In addition, decision making authorities should also be tied to role descriptions for crisis managers.

Management Group	Destroy Sensitive Material	Destroy Hard Drives and Soft Copy Materials	Destroy High-Value Materials	Increase Security Posture	Sanction Explosive Clearance Resources	Sanction Medical Emergency Support	Stop External Project Operations	Stop Internal Project Operations	Close Down Work Site	Stop Nonessential Road Movements	Stop Essential Road Movements	Stop Air Transportation	Mobilize Quick-Reaction Force	Request Assistance from Military	Request Assistance from Police	Request Support from Embassy	Evacuate Nonessential Personnel	Evacuate Essential Personnel	Evacuate Full Project	Sanction Air Evacuation Resources	Provide Local Media Statements	Provide International Media Statements	Alarm State Black and Red	Alarm State Amber	Alarm State Amber	Alarm State Local Green and Green
• Local Manager															✓		✓						✓			
• Local IRT							✓						✓	✓	✓		✓						✓	✓	✓	✓
• Project IRT				✓		✓	✓						✓	✓	✓		✓						✓	✓	✓	✓
• Program IRT	✓		✓	✓		✓	✓	✓	✓	✓			✓	✓	✓		✓	✓					✓	✓	✓	✓
• Country CRT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓
• Corporate CRT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
	Destruction			Security			Operational Activities						Support				Evacuations				Media		Alarm States			

EXHIBIT 1.11 Decision and Authority Matrix

Structuring Business Continuity Management Plans

In order to understand how the IMP should be structured and where it fits within both the corporate and field risk management and crisis response policies and plans, it is important to understand that the IMP forms one of many components of the company's Business Continuity Management Plan—effectively supporting the first response steps of the plan. More comprehensive policies and plans designed to manage the subsequent stages of a crisis will invariably be undertaken by experts within appropriate fields, typically involving more complex and event tailored approaches. The Business Continuity Management Plan itself should be a logically structured policy and procedural document designed to assess and address risks in a systematic and pragmatic manner, dealing with both theoretical and tangible requirements.

Companies might wish to consider the development of their Business Continuity Management Plans with two key aspects in mind—layers and levels:

1. **Layers.** Layers might be considered in terms of organizational or management bands within a group, from corporate to country to program to project. Understanding how a company is layered in both management and operating terms will enable the plan to reflect the organizational structure and the unique and common requirements within each management or user category.
2. **Levels.** Levels might be considered in terms of management applicability, whether strategic, operational, or tactical. Strategic interests might encompass market value, reputation, and image as well as the holistic issues a company might face. Operational issues might relate to how a company conducts business or undertakes work functions. Tactical considerations might be the granular-level aspects of how specific work packages or crisis management functions are done.

Companies will structure and layer their plans according to the nature of their industry, the complexity of their organization, and the manner in which they conduct business. However, companies may find value in structuring their plans in a consistent manner, changing only the level of detail as the plan is designed for different levels of management, or for different groups within a wider organization. Consistency ensures that a standard approach to risk and response management is achieved, and that managers moving between different parts of the company understand where information is contained, and how general practices are undertaken. This should not detract from the requirement to tailor plans to suit unique operating conditions or local requirements, but should provide a common framework for sound management application, as would be found within health and safety management approaches. Different layers will also overlap as the Business Continuity Management Plan acts to fuse the complex policies, protocols, and plans found within an organization into a unified management system. Where possible the company should seek to avoid duplication and redundancies by creating umbrella information that might apply to all aspects of the organization, while creating pillars of similarly structured, yet tailored plans for different divisions or geographic regions, as illustrated in Exhibit 1.12, Layering of Business Continuity Management Plans.

All layers of the plan should be engineered to fit in at critical junctures, especially between corporate, country, and project levels, so that the Business Continuity

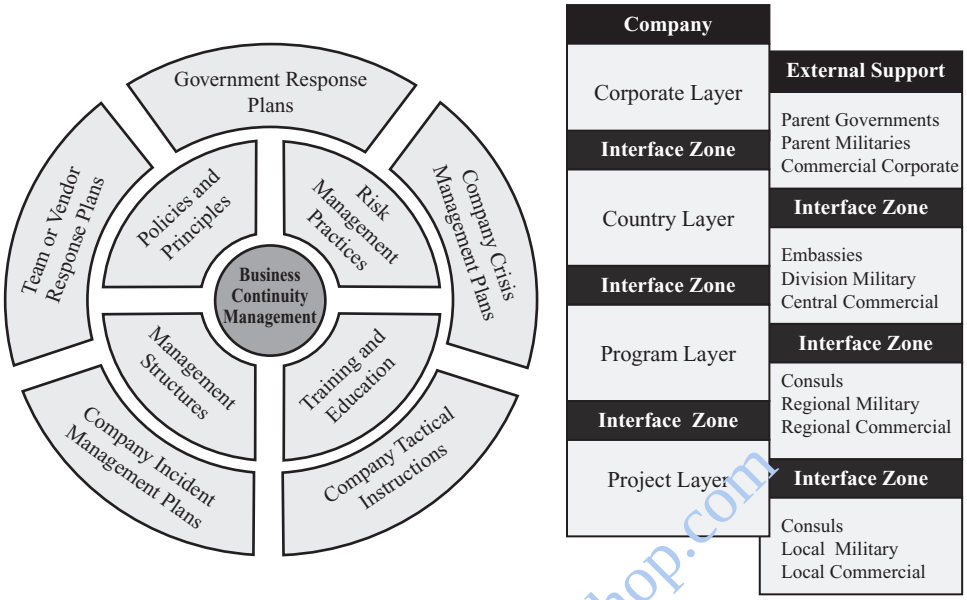

EXHIBIT 1.12 Layering of Business Continuity Management Plans

Management Plan has complementary and supporting components or layers, as illustrated in Exhibit 1.13, Convergence within the Business Continuity Management Plan.

Typically the company (or subcontracted) risk and security manager will work with the multiple stakeholders within the organization to provide a Business Continuity Management Plan that ensures that a business activity (or indeed overall

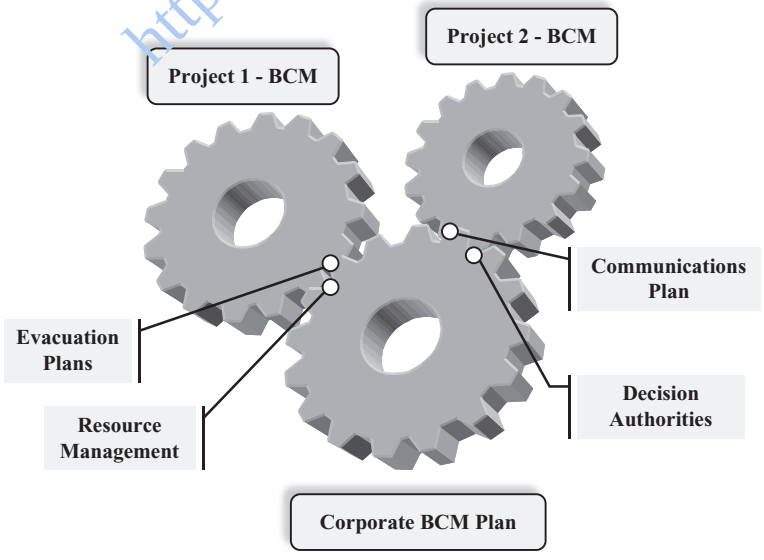

EXHIBIT 1.13 Convergence within the Business Continuity Management Plan

corporate operations) is planned within the context of risk, can operate most effectively, and exposes the company to lowest levels of threat possible. Typically, a Business Continuity Management Plan is designed to work in a logical and often chronological sequence, identifying dangers through risk assessments and deciding whether to countermand the risks with personnel or resource allocation (or whether to adopt a risk avoidance policy), before implementing the delivery of security and response measures, in all their forms, to ensure that the probability of the risk occurring is reduced to acceptable levels or dealt with most effectively. Alternatively the first stages of risk evaluation may deter a company from entering into new businesses if tolerances are breached. No organization can prevent all crises, but every organization can lower the odds of their occurrence, lower their costs, and lower potential crisis-related condemnation.

The Business Continuity Management Plan should be aligned with three basic areas of consideration, as illustrated in Exhibit 1.14. The company or contracted vendor risk manager should consider what range of risks face the company and how the company wishes to manage these risks. Risk managers should only then write policies and plans that are aligned with the considerations of contingency planning and crisis response, which include the IMP. It is important that such evaluations are not written in isolation, or from the perspective of a single risk manager, but brings together multiple stakeholders and expertise. This forms the preparedness or contingency planning aspect of risk management: where a company can reduce risks before they occur, with preemptive planning to allow the company to best manage risks prior to an event—into which the IMP will fit as a practical response component. The Business Continuity Management Plan should then consider how to address the immediate crisis requirements that typically affect the people, resources, and business goals of an affected activity, as well as how the risks pose an *impact ripple effect* on other aspects of the company's operations and business interests. It is at the immediate point of crisis that well-planned policies and procedures reduce the impacts of the risk event by managing the risks through well-defined response methodologies and training—again in which the IMP plays a key role. Finally, the Business Continuity Management Plan activities continue until all aspects of the risk event have been completed, and where both project and corporate managers have had the opportunity to review which areas within the plan were effective, and which need to be improved, modified, or augmented, allowing a company to recover effectively from a crisis. Business Continuity Management Plans should be

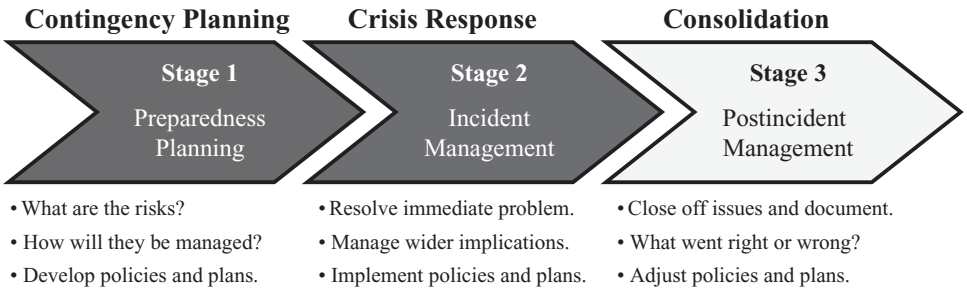

EXHIBIT 1.14 Business Continuity Management Plan Considerations

considered live documents and should be continually adjusted and validated to suit changing influences and operating practices, as well as when improved or new concepts and efficiencies are identified.

In terms of providing a framework for the risk management process, risk managers should have the three principle areas of consideration in mind when developing the four elements that comprise the Business Continuity Management Plan: the risk assessment, the contingency plans (including the IMP), crisis management, and the postincident review, as outlined in Exhibit 1.15, The Risk Management Process.

The IMP falls within both the contingency planning and the crisis response components of the Business Continuity Management Plan—designing policies, plans, and guidelines in order to prepare an organization for a crisis event, as well as then using such policies and procedures to manage the crisis response itself, especially during the early response stages of an emergency.

The Business Continuity Management Plan and its constituent components may involve the development of new corporate policies to meet strategic and complex issues, as well as bring convergence to often amorphous, dispersed, and disjointed organizations. The Business Continuity Management Plan may also address project planning procedures and tools, as well as employee education, and may require specialist support for conceptual development and plan structuring. Plans will also include executive officers, project teams, security or risk elements, legal and public relations input, monitoring groups, and administrative resources. In many cases,

EXHIBIT 1.15 The Risk Management Process

Area	Explanation
Risk Assessment	*Warning signs and analysis prior to a crisis event*. The value of a risk assessment as a diagnostic tool is measured in terms of accurate intelligence, specialist knowledge, and an achievable and pragmatic set of procedures to reduce the probability of a risk occurring.
Contingency Planning	*Preparation and prevention phase*. Contingency planning refers to measures implemented to prevent recognized or speculated serious events or emergencies. These possible activities should be identified during the risk assessment.
Crisis Management	*Incident response, damage containment, and recovery period*. Crisis management is the response to a problem while it is occurring or after an incident, utilizing the contingency planning measures, as well as the organization being able to respond quickly and effectively to unique requirements.
Postincident Review	*Review and modification of the risk management plan*. The documentation of all incident information should be conducted to support adjustments to existing policies and plans, as well as to identify shortfall within crisis management policies and management teams, in order to mitigate future crisis impact levels.

Source: Michael Blyth, *Risk and Security Management: Protecting People and Sites Worldwide*. Copyright © 2008 John Wiley & Sons. Reprinted with permission of John Wiley & Sons.

external agencies may also be involved, requiring security clearance, access to sensitive information, the formalization of contractual agreements, and the monitoring of the contract's standards. At the lower levels, basic instruction on how to use the IMP is required to ensure that it operates within the framework of the Business Continuity Management Plan—and is effectively implemented during times of need.

When the company has contracted other groups to support its business activities, whether within the project activity or as a security component, the company should consider providing, and receiving agreement on, policies and plans to enable all groups to act in unity to best respond to risk events. Without a degree of uniformity, the response will typically be disjointed and confusing, increasing the risk impacts. The IMP should be designed in such a manner to complement and support the Business Continuity Management Plan as a whole, providing information to enable sound decision making, as well as bringing initial crisis situations under control to reduce the initial and longer-term risk impacts, as well as support better business recovery. The IMP should be linked at certain points to other elements of the Business Continuity Management Plan, but might also be engineered to be able to operate as a stand-alone document where necessary. The IMP in this sense enables the transition of crisis management from nonspecialists to risk and security professionals more effectively, as well as bridging the gap between incident management protocols and crisis management plans.

Resourcing

Resourcing of Business Continuity Management Plans must occur at different levels, from strategic support from stakeholders and key decision makers to ensuring that the correct management and technological infrastructures are in place to enable the plans to be operationally effective. The design and development of Business Continuity Management Plan will be labor intensive, and consideration to contracting external consulting support should be given in order not to distract security directors or busy managers from their primary tasks. Training and practice should also be a component of resourcing, as without education and awareness of how the plan operates and interrelates with internal and external groups it will be limited in its value. The implementation of the plan should also be measured and validated at strategic design points, ensuring that it is aligned with the company ethos and operational needs. Resourcing can also be in terms of:

- **Management Capabilities.** Ensuring that the correct management expertise is applied to the plans, both for design and for implementation.
- **Specialist Support.** Ensuring that the correct expertise is applied, rather than attempting to use inappropriate and inexperienced management as a cost-false saving measure.
- **Retained Specialist Response Teams.** Establishing retainer-based expertise to deploy immediately to affected regions as the link between corporate and field management.
- **Technology and Communications.** Ensuring that effective technology supports the management expertise in the execution of their duties.

- **Risk Management Assets.** Ensuring that the correct resources are available to support risk management teams, especially special response teams.
- **Security Structures and Assets.** Ensuring that an appropriate level of security structures, as well as manpower, is in place as a mitigation measure.
- **Redundancy Measures.** Ensuring that communications, information technology (IT), and operational redundancies are in place should primary measures or facilities be affected by the crisis event.
- **Translations.** Where necessary, materials should be translated into the different user languages to ensure that incident and crisis managers can fully understand instructions and guidance offered. Documents should be translated in dual nature in order to ensure consistency and document control.

Resourcing can be considered as a range of components meeting conceptual, operational, and tactical needs. The following provides some examples of resource principles a company might wish to consider when evaluating the resources required to support their Business Continuity Management Plan:

- **Strategic Resources.** Ensuring that management support is provided to enable plans and managers to be effective.
- **Design and Development Resources.** Allocating sufficient budgets and focus to ensure that plans are designed to be reflective of the company's requirements.
- **Operational Resources.** Ensuring that the correct level of expertise is provided to enable plans to be implemented to standard.
- **Technology Resources.** Ensuring the correct technologies are provided to enable command and control of a crisis situation, as well as information flow.
- **Tactical Resources.** Ensuring that the correct equipment and training are in place to support the Business Continuity Management Plan.
- **Quality Assurance Resources.** Ensuring that adequate auditing and validation budgets and focus have been applied to ensure plans and training are kept current.

Companies will develop a Business Continuity Management Plan that meets the particular needs of their organization, or that reflects senior management or outsourced consultant design preferences. The time, money, and resources invested into the Business Continuity Management Plan will also define its structure and complexity. The Business Continuity Management Plan will typically include the elements illustrated in Exhibit 1.16, and may be considered in terms of strategic policies, plans, and considerations—the higher-level and corporate umbrella aspects of the plan, as well as the functional or response aspects. The structure of the plan will also be derived from the nature of the risks and their impacts upon the organization in order to ensure that the plan is meaningful and correctly focused on the company's unique requirements, as well as common operating considerations.

Companies should also consider methods by which to improve the sustainability of a Business Continuity Management Plan and its components with the greatest amount of ease. Often such plans quickly become redundant as the risk environment changes, personnel move, and business or project operations progress. Companies

I. Policies and Principles

- Corporate Ethos and Guiding Principles
- Corporate Operating Practices
- Corporate Communications Policies
- Corporate Procurement Policies
- Corporate Public Relations Policies
- Corporate Information Security Policies
- Special Relationships and Agreements
- Corporate Insurance and Liability Policies
- Organizational Minimal Security Standards Policy
- Corporate Due Diligence and Duty of Care Policies
- Supporting Practices and Policies
- Transfer of Critical Operations
- Contracting Supporting Agency Policies
- IT and Critical Records Management

II. Risk Management

- Corporate Risk Tolerances
- Strategic Overview of Risk Natures and Types (Risk Log)
- Strategic Corporate Risk and Impact Mapping
- Strategic and Regional Risk Evaluations
- Program Risk and Impact Mapping
- Strategic and Tactical Risk Mitigation Policies
- Strategic Risk Management Plans and Systems
- Organic Resource Management Plans
- External Resource Management Leveraging Plans
- Intelligence and Threat Analysis Reviews
- Security Surveys, Plans, and Audits
- Resource Management Planning Systems
- Training and Educational Programs
- Strategic Business Recovery Planning Measures
- Risk Tracking and Alert Systems
- Business Solution Architecture and Concept of Operations

III. Management Structures and Policies

- Corporate Organizational Structure
- Crisis and Incident Management Structure and Appointments
- Decision-Making Permissions and Matrixes
- Alert States and Trigger Response Plans
- Communications Plans and Systems
- Procurement Management and Systems
- Public Relations Management and Procedures
- Strategic Resource Management Plans
- Security and Intelligence Management Structures
- Organizational Interface Plans and Systems
- Special Agreement Management Plans
- Quality Assurance Policies and Plans
- Contracts and Relationships
- Critical Materials Management Instructions
- Contracted or Retained Specialist Support
- Response Capabilities and Times
- Business and Project Initiation Policies and Plans
- Facility and Approach Hardening Policies and Plans

IV. Tactical Instructions and Plans

- Standard Operating Procedures
- Travel Policies and Systems
- Tactics, Techniques, and Procedures
- Security Orders and Instructions
- Training and Educational Measures
- Facility Security Plans
- Procurement and Resource Management Instructions
- Reporting and Record Keeping
- Postincident Reviews
- Mapping and Schematics
- Medical Policies and Instructions
- Critical Materials Handling Instructions

V. Incident Management Plans

- Corporate Policy Flow-Downs
- Incident Management Plan Objectives
- Crisis Management Structures
- Crisis Management Roles and Responsibilities
- Decision Matrixes and Authorities
- Organizational Interface Plans
- Communications Instructions and Verbal Reporting
- Organic Resource and Leveraged Resource Instructions
- Alert States and Trigger Response Plans
- Threat Types and Overviews
- Response Information Collection Templates
- Incident Management Plan Risk Assessment Reports
- Destruction Plans

VI. Crisis Management Plans

- Evacuation Plans
- Business Recovery Plans
- Disaster Response Plans
- Kidnap and Ransom Response Plans
- IT Crisis Management
- Medical Response Plans
- Repatriation Plans
- Public Relations Crisis Plans
- Pandemic Management Plans
- Industrial Accident Management Plans
- Fraud or Corruption Management Directives
- Threats and Extortion Crises

EXHIBIT 1.16 The Business Continuity Management Plan

should attempt to broadly define which elements of the plan are static, semistatic, and fluid:

- **Static.** Information that rarely changes and is commonly centered on policy, education, or advisory information.
- **Semistatic.** Information that changes only periodically and may include significant resources, agreements, or project locations.
- **Fluid.** Information that may change on a frequent basis, including personalities, short-cycle work packages, and transition factors.

Where possible, semistatic and fluid information should be captured within tables and other informational inserts that can be replaced with ease. Placing semistatic or fluid information into the verbiage of the document can make revisions difficult, costly, and time consuming.

Where a Business Continuity Management Plan addresses various levels of a company's activities (corporate, country, and program), materials should be structured in a consistent manner, removing elements that might be redundant or not applicable. By designing a framework that can be used for each layer of need, organizations can better manage and utilize such plans. In addition, components of the plan can then be migrated to new business activities with significantly less effort than is required to repeatedly create new plans or policies.

The company should ensure that strategic and tactical elements are fused and coordinated where appropriate, and that regional tailoring occurs to reflect the nuances of a particular operating environment—without changing the structure or themes of the original plan. In addition, the company should determine where outside support plugs into the Business Continuity Management Plan, again coordinating integration to avoid friction or confusion when the policies and plans are implemented.

Design and Development

The development and design of a corporate Business Continuity Management Plan is an important aspect of how a company prepares for and responds to a crisis event. While a risk or security manager may write a Business Continuity Management Plan for a specific individual or business group, often this plan will be shared among multiple divisions and parties, spanning various levels and areas of an organization. At times the plan may also be used by supporting agencies outside of the company. Therefore, the plan should be developed to meet the needs of a wide and multitalented user audience. Often some policies and procedures already exist, and plan development should seek to incorporate these and mature or augment them, rather than reinvent the wheel and fail to exploit existing materials.

The Business Continuity Management Plan is also a living document that will grow and adapt to suit the changes in the company's approach, methodologies, and objectives, as well as the risk environment in which the plan operates. Additional contributions may be made to enhance components of the plan at various stages of its life. The plan should be configured to readily accept and incorporate additional elements; this is often achieved by compartmentalizing the plan, where appropriate, so that components can be changed, rather than requiring an entire plan update.

Identifying *data migration points* is a useful exercise, as it allows materials to be migrated from one document or policy into another, significantly reducing effort as well as ensuring consistency within supporting policies or plans. This is especially relevant if the same forms of information are found within a series of documents and might be shared through effective information management practices. Policies should also be developed with the concept of *live* and *static data* points:

- **Live Data Points.** The unique and particular details that represent the specifics of an operating area, task, or function and are relevant to a unique product. Also, information which may change on a frequent basis.
- **Static Data Points.** Common features and generic concepts or instructions that remain true across the spectrum of the business regardless of region or activity. Also, information which will rarely change within the plan.

By developing frameworks based on a foundation of static data points, and placing live data points into tables, graphs, maps, and other capture points where possible, significant time and resources can be saved in providing consistent and detailed frameworks to which live data points can be inserted. Where sanctioned and appropriate, it is also useful to provide generic templates for local project adaptation, saving the company (and field management in particular) considerable time and effort in re-creating response plans, which will be better spent on generating revenue.

When developing such plans, it is also important to understand that executive members of a busy commercial organization likely will not review a comprehensive plan in full; thus the manager should establish the core elements and responses within an executive summary at the front of the document to capture the pertinent points and recommendations, with detailed responses captured within successive annexes that can be accessed individually when required. Cheat sheets are also useful so that managers can quickly refer to a specific area of requirement, rather than have to sift through a volume of data. Supporting materials should also be captured in annexes or attachments to enable everyone, from executive officers to the field users, to choose which components they read, according to their areas of interest. Protecting the document from alteration is also useful should elements within the company be inclined to modify or edit sections to meet their local requirements. PDFs or Word-protecting documents ensure that the original version is more easily defined. A custodian should be appointed to ensure that the document remains consistent with the corporate directives and that those improvements and augmentations are incorporated and dispersed throughout the company.

Reporting of information is also a critical element of crisis management. Often information provided from the crisis point is inaccurate, disjointed, or poorly presented. The company should develop pragmatic and user-friendly report templates in order to ensure that the right information is captured, that it is presented in a consistent manner, and that the correct people receive the reports (see the section "The Communications Plan" in this chapter, and Chapter 6). Data call reports can capture immediate information in terms of what occurred and the immediate impacts, enabling various layers of managers to better understand, throughout the crisis event, what is occurring and so allow them to make the right decisions

and to mobilize the correct resources to control the event. Predefined formats remove the requirement to identify information needs or presentational formats while managers are dealing with a problem. Examples of such reports are illustrated in Chapter 6.

Corporate leaders will invariably require another layer of information (outside of the succinct data capture reports) in order to determine strategic or macro-level operational requirements that will influence corporate decision making during and following an event. Company management, as well as supporting vendors, should seek to proactively identify business continuity considerations as well as how the company may wish to proceed in terms of risk assessment validations and postincident audits. The template in Exhibit 1.17, Information Management: Strategic Planning, indicates some areas the company's field and security vendors should be considering during or immediately after a crisis event. Such strategic considerations are typically fed from the initial incident management reports; however, they reflect the transition from incident to crisis management levels and focus areas.

Companies may build business continuity management plans either from scratch or by leveraging existing policies and plans. They should seek to mature plans where possible, exploiting in-house and publicly available materials to ensure that plans are more comprehensive, to avoid duplication, and to reduce the time and effort required for design and development. In addition, maturing plans also enables more receptive implementation from users as existing policies and protocols are rationalized and put to use.

At every point within an emergency event, it is essential that information provided is as accurate and detailed as possible; assumptions should be avoided and educated assessments should be quantified to avoid inaccurate details being reported as facts. Reports should be adapted and augmented to reflect unique factors, and flexibility and innovation should be key aspects during any crisis.

EXHIBIT 1.17 Information Management: Strategic Planning

Executive Summary:
Incident Facts:

- Immediate Threat Picture
- Immediate Threats to Personnel/Business
- Immediate Response Requirements
- Sustained Response Requirements
- Highest-Risk Activities
- Low-Risk Activities
- Risk Review Requirements
- Recommendations
- Interim Threat Picture
- Interim Threats to Personnel/Business
- Interim Response Requirements
- Long-Term Needs
- Medium-Risk Activities
- Postincident Review Requirements
- Supporting Groups and Activities

Appendixes:

- Serious Incident Reports
- Communications Log
- Actions Taken
- Intelligence Reviews
- Crisis Team Assessments
- Policies Invoked
- Casuality Reports
- External Agency Reports
- Resources Engaged

Reported by Title Phone/E-mail

Source: Michael Blyth, *Risk and Security Management: Protecting People and Sites Worldwide.* Copyright © 2008 John Wiley & Sons. Reprinted with permission of John Wiley & Sons.

Integrated and Compartmentalized Policies

During the design and development phase of creating a Business Continuity Management Plan and associated components, it should be determined whether as a result of company ethos or corporate or operational circumstance the policies and plans being developed will be part of a broader and integrated management system, or whether they may need to operate independently and autonomously from each other. While ideally all policies and plans should be supported and work as part of an integrated system, at times an organization may allocate responsibilities for various elements of the management of risk to different divisions, and under those circumstances it may be challenging to align some of the higher-level strategies, systems, and policies across a complex and geographically and organizationally disjointed corporation. Under these circumstances, managers should develop policies and plans that are largely complete within themselves, rather than having core components for the effective operation of a particular plan be held within another document, which they may have no input into or control over.

Integrated policies and plans will typically have decision matrixes, alert states and trigger response plans, and other such elements within overarching policy documents, rather than run the risk of repetition and error within individual risk management policies and plans. From the overarching policies such elements may be migrated downward so that consistency of approach is reflected across different levels of the Business Continuity Management Plan. When organizations choose to have individual groups or divisions defining their own strategic, operational, and tactical approaches, there may be no option but for individual managers to define their own core approaches in order to ensure that their part of the contingency planning and crisis response organization is complete and effective. Ideally the fusion of multiple requirements is captured within a single corporate officer (typically the chief security officer) so that repetition is avoided, consistency is adopted, and synergies and efficiencies are identified and implemented.

Reporting and Record Keeping

Writing up the details of a crisis incident is essential to ensure that accurate facts are recorded and maintained, and that information for any subsequent internal review as well as possible government or civil audits or insurance and liability claims are presented in a fashion reflecting the company's policies, ethos, standards, and objectives. Any documentation provided to external persons or groups should also be reviewed by the country crisis response manager (at a minimum) prior to being released, as poorly worded reporting can cause a wide spectrum of issues for the company and its employees. Accurate and correctly worded reporting is also critical to ensuring that insurance for any injured person is awarded. Information should be held by an appointed custodian so that materials can be easily and accurately retrieved when required, often months or years after an event.

Implementing the Business Continuity Management Plan

The Business Continuity Management Plan must be supported at every level in order to be successful. At the corporate level, a risk policy strategy needs to be

agreed on and distributed to appropriate key decision makers and groups, providing a framework for systematically developing risk assessments that corporate and program management can use to guide their activities and focuses. These in turn contribute to the focus and subsequent development of the IMP, should they not already be in place. At the program level, the plans must be usable and reflective of realistic conditions and responses. Synergies and interfaces between corporate and program-level plans and responses should also be identified and integrated to ensure that corporate and project teams do not work independently of or in isolation from each other, but undertake concurrent and complementary activities. Some of the following principal values should be considered when developing the Business Continuity Management Plan:

- Provide a convenient framework for developing a quantitative risk assessment that prioritizes both the goals and the objectives of the company in the context of the associated risks or threats.
- Provide a systematic and repeatable method for evaluating an organization's risks using the best threat information available. Seek efficiencies by drawing on existing templates and formats.
- Permit program, project, and other key managers the opportunity to identify their departmental and organizational risks.
- Identify information gaps in order to establish a better risk picture.
- Allow risk and security managers to express their expectations about the consequences of the postulated incident types, and elicit their observations and recommendations on how to mitigate or respond to these risks.
- Allow business leaders and project managers to review the risks and comment on how risk management policies, approaches, and plans might affect program design, objectives, and goals.
- Provide insights into how the uncertainty of managers' expectations affects the prioritization of risk or security requirements. Allow risk models to be easily updated with new input data.
- Develop a spectrum of policies and plans in order to reduce the likelihood of the risks occurring, as well as to effectively manage an event should it occur.
- Permit stakeholders to review and comment on the policies, plans, and procedures and adjust and improve where necessary, thereby gaining greater group buy-in.
- Train and test both the plans and managers in their use and applicability.
- Support market entry design with risk, business, and project managers working in collaboration with each other.

Risk management should be cyclic in nature, with continuity between the users (projects) and managers (corporate). In addition, the process is also cyclic in terms that the business need prompts the risk assessment, which feeds business decision making and associated policies and plans, with events driving modifications, which then influence business needs and decision making, as illustrated in Exhibit 1.18, Risk Management Cycle.

Risk information needs to be shared with appropriate groups and individuals in order to ensure that a rounded understanding of the risks is gained, and that mitigation measures (including the IMP) are most effective. Information sharing can

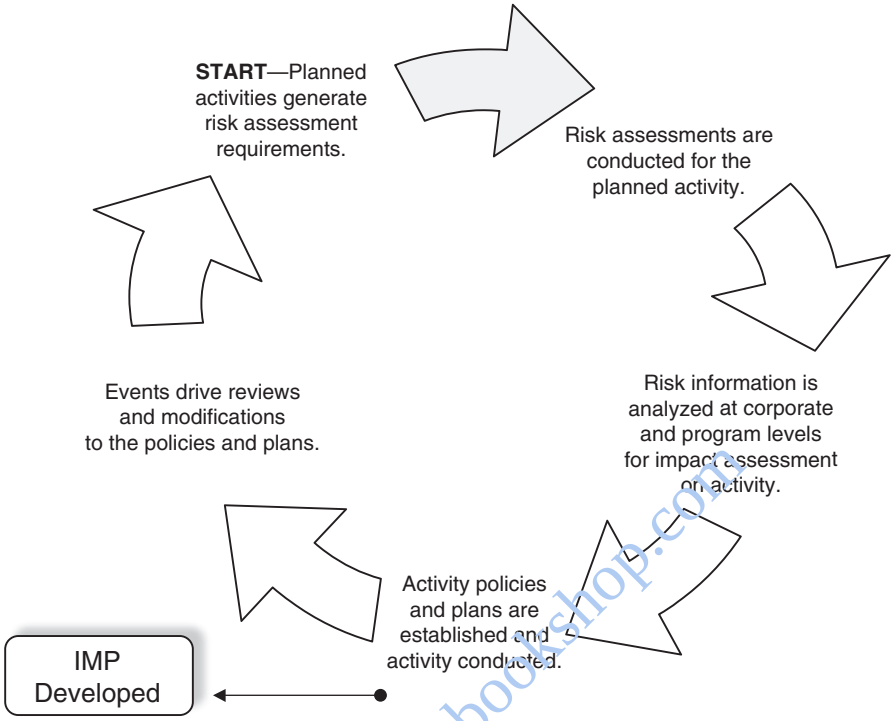

EXHIBIT 1.18 Risk Management Cycle

Source: Michael Blyth, *Risk and Security Management: Protecting People and Sites Worldwide.* Copyright © 2008 John Wiley & Sons. Reprinted with permission of John Wiley & Sons.

be through training, warning posters, leaflets, or daily intelligence briefings, which highlight specific risks or risk environments. The policies and procedures used to mitigate risk are a reflection of the requirements identified within the Business Continuity Management Plan. Dependent on the size, nature, and diversity of the organization, the procedures can vary from simple and pragmatic brochures to volumes of complicated manuals and training exercises covering a multitude of subjects. Some of the generic procedures that should be included within any organization are the establishment of a company mission statement, general policy documents, personnel training requirements, and monitoring and validation techniques (internal and external). The identification of resource requirements (supported by appropriate budgets) is also essential to ensure that a Business Continuity Management Plan can be established, and effectively implemented and sustained.

The following sections describe the elements of the Business Continuity Management Plan.

POLICY DOCUMENTS All risk management policies should be periodically updated to reflect the current intelligence-driven threats, as well as the influences that any particular operating environment or activity may have upon the company and its procedures. All personnel should be informed of the current sources of risk, with

appropriate details pertaining to how the risks might impact the organization, as well as the measures taken to address them. In order to ensure that all implemented measures are effective, an established Security Management System, or set of standard operating procedures (SOPs) can be used to guide daily activities in mitigating risk. The incident management plan (IMP) then supports managers in bringing any resulting emergency situation under control. These policy documents can be engineered at both the corporate and field levels and should also provide general guidelines on how to activate the incident management and crisis response teams, how individuals are expected to respond to an incident, who they should inform, and what other assets are available to support them. It is often useful for policy documents to be accompanied by relevant training and exercises to ensure that the policies are clearly understood and thoroughly rehearsed.

REPRESENTING INFORMATION The ability of managers to understand the information being represented is defined by the manner in which data is structured, delivered, and presented. This is as important for both those attempting to understand and use the Business Continuity Management Plan and those attempting to gain support and buy-in from corporate and project leadership when developing the plans. Often information that is unstructured and poorly presented devalues critical information contained within the text. Simple techniques and systems of representation can make information easier to digest, as well as provide concise and logical frameworks for more effective delivery.

Companies should seek logical and succinct methods by which to capture and present information to the stakeholders and users of Business Continuity Management Plans so that well-structured and logically presented documents can be developed and consistently used. Consideration should be given to design a consistent framework for such policies and plans, enabling repeated use and reducing repetition and redundancies where possible. Professionally and logically presented materials also inspire greater confidence within a group and increase the likelihood that managers will read, understand, and use the guidance provided.

TRAINING Training and rehearsals provide the most effective method by which to instill confidence in first responders and crisis managers, as well as create the crucial instinctive responses required of personnel when facing the common threats posed to people, an activity, or organization. Corporate and project management education and training are useful tools to run the crisis response plan through its paces. This is usually done through short seminars, training sessions, or desktop exercises, which require little resource support and focus on key decision makers and how they undertake their individual roles, as well as how they fit within the wider organizational structure. Technical and practical training may also be required in order to use the wide variety of equipment and personal skills necessary to meet the measures identified in the risk assessment, sanctioned in the Business Continuity Management Plan, and implemented in the risk management procedures and incident management plan. Training agencies should be selected according to their expertise and experience, with continued training requirements identified to prevent *skill fade*. Training should also include relevant outside agencies and independent monitoring assessors to ensure that the measures used are current and effective, and regionally oriented. The use of desktop exercises and practical training

can also help focus management teams at different levels, at relatively low cost to the company.

The company should also not lose sight of the need to ensure that vendors, subcontractors, or teammates, whom the company may be responsible for or reliant on, are also appropriately educated and trained. Companies may opt to include such training as an element of a security vendor's contract—incorporating training or education of company staff as part of a preselection or predeployment requirement. This is particularly relevant in remote or challenged environments where a security management element can concurrently bring training value to the company.

Training plays a crucial part in ensuring that the crisis response plans can be effectively utilized during an event, and educational packages can include management and personnel crisis response training, tactical procedures and emergency response drills, first aid, hostile environment training, and situational awareness training. The company should consider whether a vendor might also bring other skills to supplement its own training regimes and incorporate these into any training cycles. This additional element of service can be especially relevant where certain skill sets, such as first aid in Africa or cross-decking (i.e., moving from one vehicle to another during an incident) in Iraq, might be useful for company personnel to receive instruction on. Either the vendor or the company should document training program attendance and adjust other service area expectations to account for time expended on developing and imparting vendor-to-company training packages. Training records also evidence the company's efforts to minimize risk following an incident, or during an investigation or audit.

Often training is set within unrealistic conditions, without the chaos, confusion, erroneous reporting, and unpredictable responses that typically accompany a crisis situation. Training and evaluating managers should insert errors, confusion, and other debilitating factors within training exercises to create a realistic atmosphere for crisis management response. Should these problems not occur during actual crisis events, the crisis management team will typically respond better, having undergone more challenging training and exercise scenarios. The adage "plan for the best, train for the worst" will best support preparation of responding managers. Training should however always be positive in nature.

The company should also seek to capitalize on staff expertise to strengthen all professional categories within a contract. Training regimes should be in place not only to meet stipulated needs but also to expand or strengthen professional competence into supporting areas, where appropriate. Companies should seek areas in which vendors can, over time, further enhance service delivery through an expansion of staff skills sets, whether they are management capabilities or more practical skills. Training can also play a part in a socioeconomic plan whereby local employees receive sustainable employment training to better their economic situation as well as their community. For sustained operations, a "train the trainer" scheme is also highly beneficial in building up a broad base of capabilities within a project team or local workforce in order to reduce the effects of a crisis event.

COST JUSTIFICATION It is often difficult to gain support for the allocation of budgets to risk management, as costs may be spread across multiple business units with no clear delineation or evidencing of value. Often companies will seek to place risk management and security within a commercial context, aiming to minimize cost

while increasing service delivery as a result. Risk management is commonly viewed as a cost center, with no identifiable or tangible benefits to the business unit, but a clear cost to the project's bottom-line profits. Justifying the investment of fiscal resources to developing a Business Continuity Management Plan and associated subplans such as the IMP can be a difficult part of the risk manager's function, especially when risk is based largely on professional judgment, rather than evidenced fact.

A historical cost analysis of known crisis events can illustrate risk impacts to business or project management, as well as provide a basis for cost analysis. In addition, if operations have been ongoing within a region by the company, or similar companies, a historical trend analysis of risks as well as security costs can be developed. Corporate risk tolerances and the experiences and expertise of corporate leaders will also define the approach and cost acceptance for effective risk management. To support the justification for investment in plan design and the engagement of risk policy consultancy, or the internal focus needed to create policies, plans, and procedures, companies should seek to develop systems that can be quickly and effectively realigned to meet new business or project requirements, demonstrating their versatility in terms of being used repeatedly to support company diverse needs. The development of one-time use policies, procedures, and plans might be required for unique projects; however, more frequently retailoring can be undertaken using (initially) well-developed materials—demonstrating utility and an increased value of such plans.

CRISIS MANAGEMENT TOOLS Contingency planning should include developing tools and mechanisms that enable the flow of accurate information as well as authorized decision making and resource allocation to support the management of a crisis event. Communications plans, decision matrixes, procurement and resource plans, and other tools and policies will support a crisis team to bring control to an event quickly and effectively. Thought should be given to designing effective tools by which to meet as many concurrent and pan-dimensional aspects of the Business Continuity Management Plan as possible.

Reference Mapping One aspect of representing information is through reference mapping. The management of a crisis at a single site is difficult under the best of circumstances, but crisis management becomes significantly more challenging when there are numerous sites involved, or when a crisis management team is seeking to control an incident response of a remote or unfamiliar location. An effective way to annotate critical locations and routes, as well as specific areas of interest, quickly and efficiently is to create project site or work area grid overlays. Such overlays allow for the immediate identification of a problem area or control point during emergencies, whether the threat comes from industrial, criminal, or natural sources. Such tools also facilitate process interfaces between the project and the executive crisis teams, as well as with supporting military, law enforcement, or civil agencies. The overlays for a specific project should all use the same scales, symbols, and numbering systems to ensure consistency. Exhibit 1.19, Project Site McKinsey Area Grid Overlay, provides an example of a simple project grid overlay. Integration with supporting groups, both in-house and external, needs to be done as early as possible in the planning process and should include the locations and routes for external groups to meet with project site groups (especially incident control points), or by

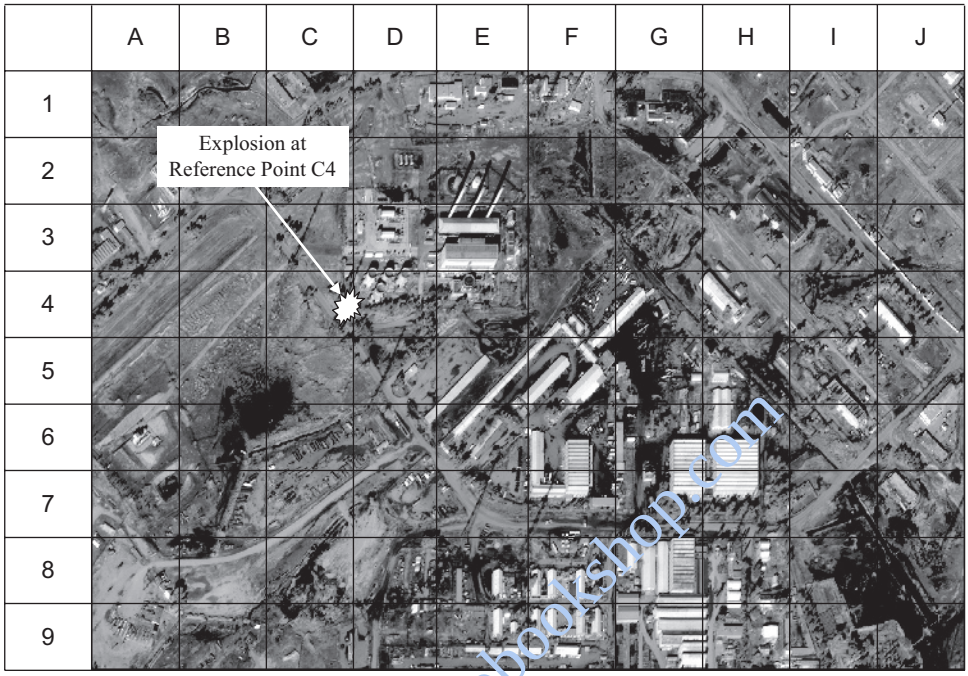

EXHIBIT 1.19 Project Site McKinsey Area Grid Overlay

which groups can safely enter the site. This form of visual representation is also useful to illustrate existing labor requirements by denoting staffing numbers by post or activity. Such tools should be used as part of the IMP reporting system.

Developing Schematics The company project or security managers (or a good security provider's management team) will be able to develop detailed and professional project site and building schematic plans and diagrams without the use of graphic artists or complex IT programs. Such diagrams can be overlays of satellite imagery or be drawn independently of such technological resources, bringing the same value as a project grid overlay to represent information more clearly to the company's executive and project teams. Such visuals provide an invaluable tool for crisis response management, as illustrated in Exhibit 1.20. Schematics and diagrams will be especially important if mapping or floor plans are unavailable or out of date. Schematics and diagrams form an important part of security documentation and should be as simple and clear as possible.

Facility structures should also be captured by the use of floor plans, as illustrated in Exhibit 1.21 using PowerPoint and Exhibit 1.22 using Visio. This is especially useful if personnel have not visited the site themselves, as it allows management to visualize the layout of the local areas and project facilities as well as attribute activities to space in advance of a visit for planning purposes. That said, often floor plans are restricted or not available. The company or a security vendor's security

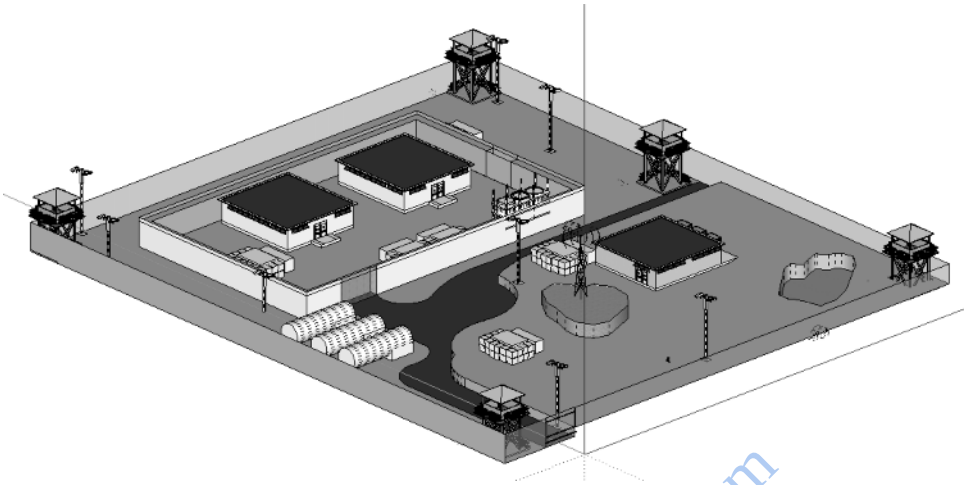

EXHIBIT 1.20 Site Schematics

manager may be required to map out building structures or layouts quickly for reports, security plans, and response protocols.

Such schematics and floor plans should be included within the IMP or associated security plans in order to provide a simple and clear method of reporting the location of a crisis event. Whether building schematics and floor designs are available or must be locally produced by managers, these tools can also be forwarded with written reports to better illustrate the location of a crisis point. Simple IT programs such as PowerPoint and Visio can enable consultants and managers to professionally and accurately present information. This will be of significant value to those crisis managers who may be remote from or unfamiliar with the layout of the affected area, allowing them to visualize the issue and place it within a geographic context.

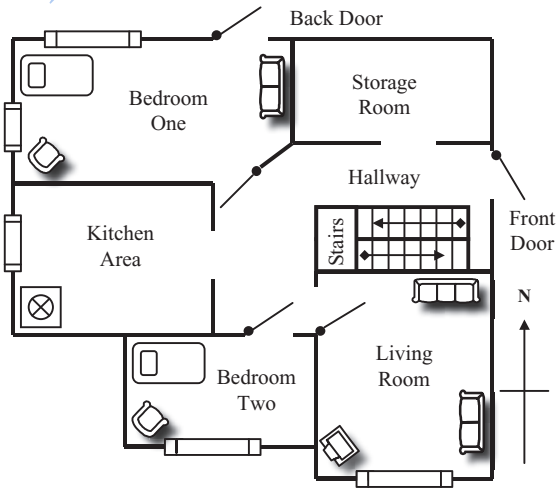

EXHIBIT 1.21 Simple Floor Plan Using PowerPoint

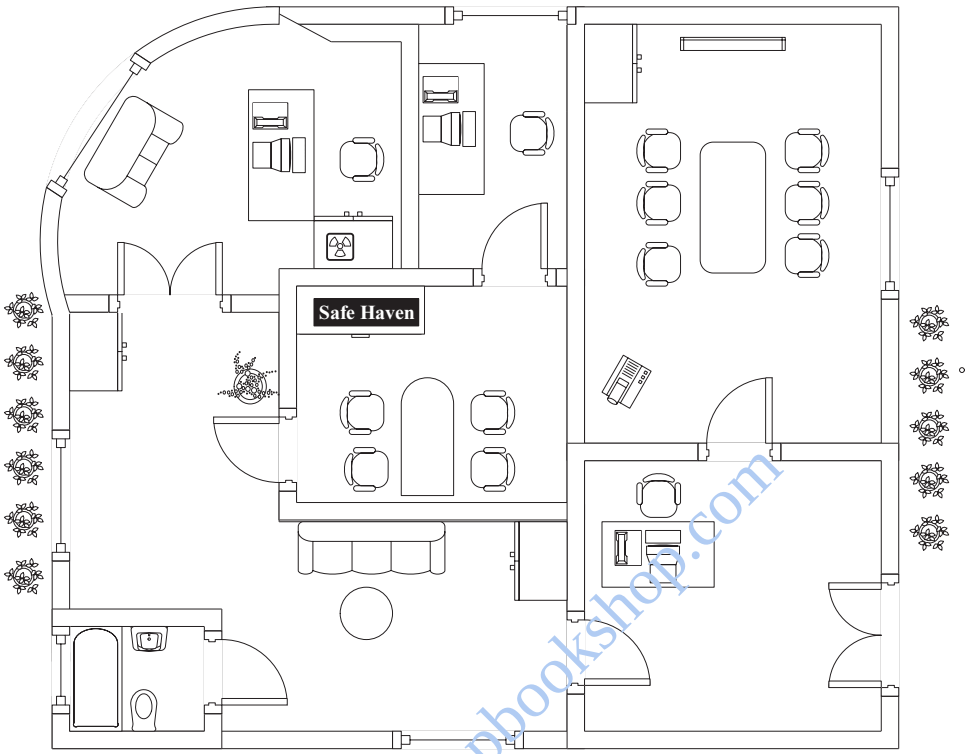

EXHIBIT 1.22 Simple Floor Plan Using Visio

SUSTAINING THE BUSINESS CONTINUITY MANAGEMENT PLAN Enterprise resilience should be a factor of the company's corporate culture. It should be used as part of general business, both in terms of market entry or business and project development planning, as well as when undertaking work. The Business Continuity Management Plan should be sustained through scheduled and event-driven audits, reviews, and amendments—without which plans will quickly become redundant and ineffective. The Business Continuity Management Plan should grow and adjust with company focuses and operations, through a cyclically driven process of understanding the organization and its goals in order to fulfill the strategic and tactical requirements of the plan—in alignment with corporate and business drivers. This will allow the focused development and implementation of the Business Continuity Management Plan measures and responses, with exercising and validating the plans on a scheduled or event-driven basis, as illustrated by Exhibit 1.23.

The Communications Plan

The *communications plan* provides the medium by which information and decisions can flow most effectively from the point or origination of the crisis event cascading or flowing to specific points throughout incident and crisis management organizations within a company. Information flow under the best of circumstances is often poor within large, complex, or geographically separated groups or organizations.

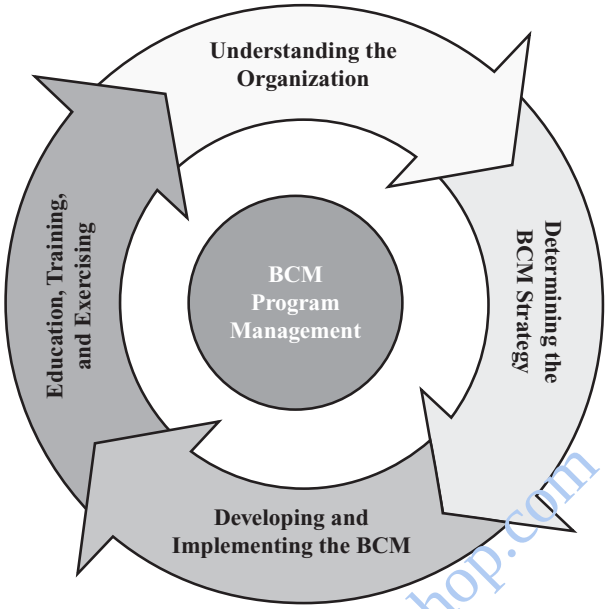

EXHIBIT 1.23 Business Continuity Management Program Management

Under crisis situations, the flow of information becomes even more disjointed and inaccurate as the event will inherently create confusion, and management is often absorbed in dealing with the issues, rather than in channeling accurate information to supporting or corporate offices. Information managers are typically those managing the incident at the field level, or the risk or security managers and directors within a company. Where multiple management elements are involved, it can be useful to designate key information managers within a crisis management organization who are responsible for collating and analyzing multiple sources of information in order to streamline information flow to appropriate decision makers and supporting groups. Where possible, multiple parties should funnel information into capture points, which then feed condensed and accurate data onward to decision makers and resource managers, as illustrated in Exhibit 1.24, Information Management Flows.

Exhibit 1.25 illustrates a simplified communications plan that can be used to support both the IMP and the broader Business Continuity Management Plan requirements. Company telephone directories are useful for capturing considerable

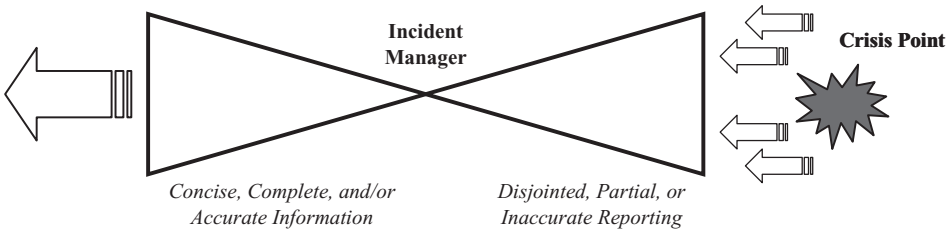

EXHIBIT 1.24 Information Management Flows

Organization	Appointment	Name	Title	Group Code	Location	Mobile No.	Office No.	E-mail	Deputy
Corporate CRT									
Company CRT	Crisis Commander	John Hopkins	CEO	**A**	Pasadena	011 - 223322	011 - 232221	Jhopkins@hillens.com	Les Dennis
Company CRT	Legal Counsel	Sid Arthan	Legal VP	**A**	Chicago	011 - 334433	011 - 192929	sartha@hillens.com	Claire Smith
Company CRT	Finance Director	Alex Rose	Finance VP	**B**	Pasadena	011 - 998877	011 - 819272	a.rose@hillens.com	Jim Donals
Company CRT	Physical Risk/Security	Craig Russel	Security Director	**A**	Pasadena	011 - 617171	011 - 929281	Crussel@hillens.com	Frank Janes
Country CRT									
Country CRT	Crisis Commander	Sal McDonal	Chief of Party	**B**	Khartoum	011 - 273828	123 - 818181	cop.power@hillens.com	Jane Mansfield
Country CRT	Logistics Manager	Jonny Walkins	Operations Maneger	**B**	Khartoum	011 - 929299	123 - 992929	opsmngr.power@hillens.com	Jack Hill
Country CRT	Physical Risk/Security	Fred Crano	Security Manager	**B**	Khartoum	011 - 929292	123 - 898282	sudansy@hillens.com	Mike Power
Program IRT									
Program—Power	Crisis Commander	Andrew Riley	Program Manager	**B**	Khartoum	123 - 4568987	123 - 589706	ariley@hillens.com	Sal McDonald
Program—Power	Logistics Manager	Brian Mavis	Operations Manager	**C**	Khartoum	123 - 002020	123 - 939292	bmavis@hillens.com	Jonny Watkins
Program—Power	Physical Risk/Security	Mick Fillis	Security Director	**C**	Khartoum	123 - 929281	123 - 887766	mfillis@hillens.com	Sid Andrews
Project IRT									
Juba Power Station	Crisis Commander	John McDonald	Project Manager	**C**	Juba City	123 - 445554	123 - 465758	Jmcdonal@hillens.com	Kevin Pillar
Juba Power Station	Logistics Manager	Sid Andrews	Security Manager	**D**	Juba City	123 - 446565	123 - 778888	Security@hillens.com	Fred Carney
Juba Power Station	Physical Risk/Security	Fred Carrney	Guard Commander	**D**	Juba City	123 - 777676	123 - 444554	Guard_cdr@hillens.com	None
Organization		**Name**	**Title**		**Location**	**Mobile No.**	**Office No.**	**E-mail**	**Deputy**
Government Agencies									
Law Enforcement	Law Enforcement	Jim Harrington	Chief of Police	**E**	Juba City	123 - 4568987	123 - 589706	Jharrington@jubapolice.com	Inspector Davis
Military Forces	Military Support	David Green	Colonel	**B**	Juba Camp	123 - 4567888	123 - 777668	Dgreen@sudan_mil.com	Major Smith
Embassy	Intelligence Support	Paul Simons	RSO	**B**	Khartoum	123 - 9909000	123 - 776545	rso@usembassy_sudan.com	Clare Williams
Commercial Support									
Medical Clinic	Medical Support	St. Francis	Emergency Room	**F**	Juba City	123 - 999299	123 - 999929	francis@emergency.com	NA
Aviation Support	Movement	FlyGreen	Operations	**F**	Khartoum	123 - 002020	123 - 939292	operations@glygreen.com	NA
Security Response	Additional Security	Shield	Tactical Operations	**D**	Juba City	123 - 929281	123 - 887766	TOC@shield.com	NA
Local Law Firm	Legal Support	McKinney	Legal Officer	**TBD**	Lagos	124 - 922292	124 - 929291	Legal.offcier@mckinney.com	NA

Information Group Codes

- **Group Code A** Personnel have access to all information relating to the incident, including corporate strategic and tactical responses, as well as liability, legal, and public relations risks. Also, all secret or sensitive information from external sources, including embassies, consuls, military agencies, federal law enforcement, intelligence services, and host nation groups.
- **Group Code B** Personnel have access to all information relating to the incident, including corporate strategic and tactical responses, as well as liability, legal, and public relations risks. Also, all unrestricted or nonsensitive information from external sources, including embassies, consuls, military agencies, federal law enforcement, and other such groups.
- **Group Code C** Personnel have access to all information relating to the incident and corporate tactical responses. Also, all unrestricted or nonsensitive information from external sources, including embassies, consuls, military agencies, federal law enforcement, intelligence services, and host nation groups.
- **Group Code D** Personnel have access to all information relating to the incident and program-level tactical responses. Also, all unrestricted or nonsensitive information from external sources, including embassies, consuls, military agencies, federal law enforcement, intelligence services, and host nation groups.
- **Group Code E** Personnel have access to all information relating to the incident and program-level tactical responses, as well as selected information provided from multi-agency-agency unrestricted sources, as it relates specifically to their area of responsibility.
- **Group Code F** Personnel will have access to selected information relating to project-level tactical responses, as well as threat alerts related to their specific appointment or function within the project.

EXHIBIT 1.25 Crisis Communications Plan

amounts of personnel and organizational contact details. However, during a crisis event a narrowed selection of contact names and details should be on hand to ensure that managers can quickly place persons against functions, and so better initiate response plans and reach out to those with the knowledge and authority to offer advice, make decisions, and mobilize support. It is important to keep such communication plans current, as a typical failing of many organizations is not to update the names and numbers listed there; frequently the majority are incorrect when the time comes to use the plan. More strategic communications plans might also be developed to apportion groups or organizations to responsibilities and functions, rather than to individuals. A communications plan may be layered and involve multiple matrixes to capture both internal and external decision makers, resources, and support. Communication plans may also be linked to decision making, interface, and resource management plans, either as separate documents or as a combined matrix.

Each crisis event will be unique and will involve changing interactions with external groups, whether they are government support organizations or other commercial enterprises. Where a company has high-profile activities, or where a crisis event is significant, the media may seek information from both the incident site and the corporate offices. Typically, program management should seek to avoid contact with the press, deferring to a nominated public relations representative. In addition, care should be taken in communicating directly with families; such activities are best conducted at a personal level rather than by indirect means, and they usually are undertaken by a corporately appointed spokesperson trained in managing sensitive situations. Companies may also seek local law enforcement support when imparting bad news to families or when seeking to prevent press access to affected families. A communications plan should seek to allocate the correct responsibilities for functions within the Business Continuity Management Plan in order to avoid well-intentioned but inappropriate communications both within and external to the company. The communications plan should also focus on how information is shared, as well as permissions and authorities for information release. Some suggested recommendations that might be part of a communications plan's information and communications guidance section follow:

- Always gather accurate facts—never pass on assumptions or speculations as facts.
- Provide an incident data call report at the earliest opportunity, and update information regularly.
- Do not liaise with the press. Direct them to the appropriate spokesperson within the company.
- Do not pass casualty details outside of incident response team(s) until approval is given by authorized management. Information on fatalities should be passed only to the corporate crisis response team.
- Close communication mediums outside of the crisis management team if required (and appropriate) to control information flow and avoid rumors or erroneous information.
- Injury and casualty facts must be accurate—names, details, extent, location, and so forth.
- Warn government agencies for possible support requirements early.

- Confirm facts again. Do this on a regular basis so that information is current and accurate.
- Alert supporting agencies as to what you are doing, when it will be done, and what you need for support.
- Conduct a local group briefing at the first appropriate opportunity in order to pass on accurate information to the appropriate contractors. Conduct regular updates.
- Write all documents and reports in a manner usable for internal and external audits.
- Collate and deliver all materials to corporate offices for review and archiving.
- Ensure that information is up to date within any plans, and test them periodically.
- Make plans simple and logical to use; avoid redundancy where possible.
- Ensure that those leaving the organization are taken out of communication plans and distribution lists.

Defining information *group codes* also may be useful, or at times necessary, to ensure that only appropriate personnel receive sensitive information. Information may need to be filtered for certain management levels, or be restricted to only those who need, or are cleared to receive, that information. There is an inherent desire for managers to have access to all information—and often understanding peripheral activities and influences does support better decision making. However, the company should ask itself:

- Is real value gained from sharing a sensitive component of information—does it really support the crisis response performance for that person to know these facts?
- What risks are associated with sharing information—does sharing this information compromise the company, information provider, or employees?
- Will the group or individual be capable of protecting that information—will they then be able to filter subsequent information sharing themselves?

Exhibit 1.25 indicates a simple table that can be used to capture the different layers of internal and external crisis management functions that might be required in order to mobilize the correct resources needed to bring knowledge, expertise, and guidance to the crisis event. Such tables also ensure that the correct personnel are advised as to the situation, supporting the channeling and flow of information to multiple groups and individuals. E-mail distribution lists and text alerts can also be developed so that primary and secondary personnel are always included in correspondence.

INFORMATION CASCADE SYSTEMS The communications plan should contain a documented information or reporting cascade system (or phone tree) to establish at the outset of a project or business activity responsibilities and communication channels for alerting management and assisting the effective flow of accurate information. Such systems can also apply to companywide response requirements. Cascade systems may involve the delivery of predetermined reports to alert company managers through e-mails and phone calls, or to mobilize internal and external resources to

respond along predefined planning measures. The communications plan should be readily accessible to those implementing the IMP so that they are able to flow information horizontally and vertically within the company, as well as draw upon the right help and resources in order to best manage their part of the crisis response measures.

Cascade systems or phone trees provide an effective medium where information flows to focal or nodal points, who then have defined persons or groups to contact. This way a clean and accurate delivery of information is achieved quickly, as illustrated in Exhibit 1.26, Information Cascade System. In addition, all contact details should be listed within an easy-to-use document to avoid confusion and make the reporting system as simple and efficient as possible. This document should also provide some basic guidelines so that simple but fundamental errors are not made by the incident response and crisis response teams during times of high stress.

Such plans should be reviewed by all managers so that they are familiar with the requirements. These documents should be placed in operations or response centers or other appropriate locations as a matter of protocol. Web-based systems can also be highly effective, unless the internet or power provisions fail. Contact details and responsibilities should be double-checked and updated where necessary, as when needed the most they are often found to be inaccurate. Senior management staff should confirm that all submanagers are aware of the requirements and guidelines and that they display these documents in the required locations. However, materials should also be protected so that unauthorized persons do not have access to contact details, names, or other sensitive details.

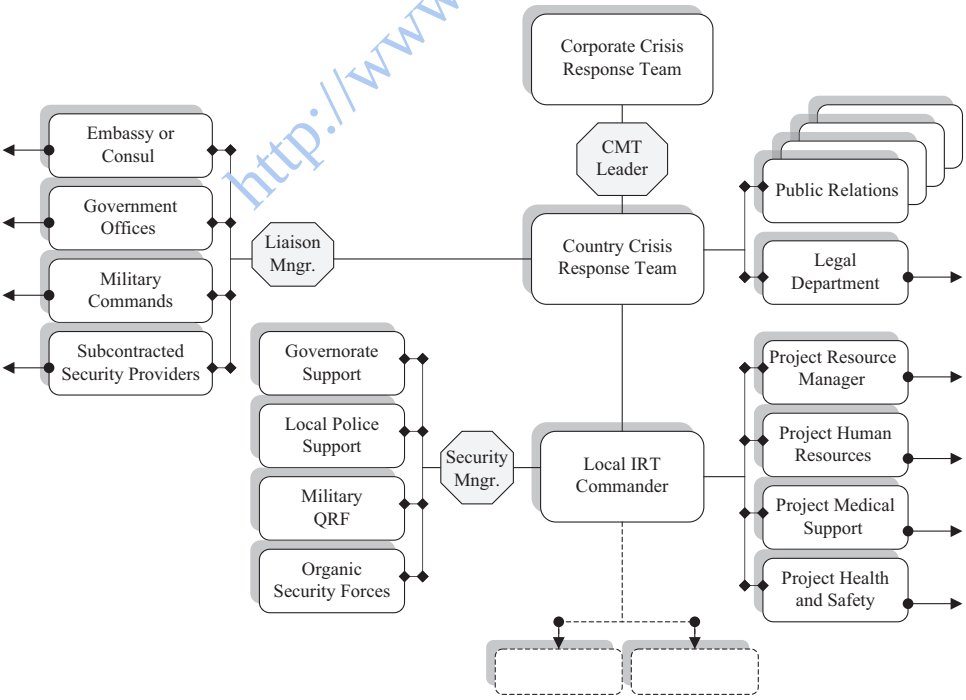

EXHIBIT 1.26 Information Cascade System

It can also be useful to annotate any particular roles or responsibilities associated with each appointment if the Business Continuity Management Plan has elements that could be considered. Companies may also wish to develop an automated messaging plan in order to text or e-mail predefined information to a wide audience, ensuring that a one-time message is delivered to a mass audience. In addition, defining an organized manner by which to impart information should support an organization's ability to cascade information quickly and accurately.

Organizational Interface Plans

Within any project environment, but especially within challenging, new or remote operating environments, it is useful for the company or its vendors to establish a network of external relationships or contacts who might be positioned to support the company in the event of an emergency. Companies should develop an *emergency management information system* (EMIS) to enable continuity and interoperability between emergency and management stakeholders. The EMIS provides the structure by which emergency plans and policies can be integrated between organic and external groups and agencies. The company (during the solicitation for subcontractors) should evaluate a security vendor's ability to draw on the strengths and capabilities of external agencies to support the company's business activities, as well as crisis response needs. The company should also seek to establish its own network of relationships in order to better position itself to operate more efficiently and respond more effectively—punching above its weight in terms of organic resources to actual capabilities.

While leveraging external resources and capabilities (either directly or via a third party) exponentially increases the company's crisis resources, it is important that the project staff and supporting vendor companies understand the parameters and limitations in which they are permitted to operate when engaging external resources to support the company. Reputational issues, corporate policies, and political sensitivities are but a few considerations that field staff may not fully take into account when attempting to find pragmatic solutions to their risk issues.

Establishing a formal integration plan (at various levels) also reduces duplication of effort between the vendor and the company, as well as limiting any other conflictions of interest when considering which agencies to approach for collaborative support agreements or memorandums of understanding (MOUs). Such elements should be included within the response guidelines of the IMP in a simplified format to guide managers to supporting groups as part of the incident management response. When using a subcontractor to support such a plan, the company should develop a policy to articulate how external agencies might be used to augment the company's business activity, and any limitations or restrictions which might apply. The following sample issues for integration consideration might be included:

- Confirm that liaison has been sanctioned by the company (and parent company).
- Confirm who is authorized to negotiate and sanction agreements, as well as the nature and scope of such agreements.
- Confirm the language to be used and the limitations imposed.
- Articulate how such integration affects the business activities, as well as any teammates or subcontractors.

- Confirm the extent of communications networking and emergency communications plans.
- Confirm the geographical proximity of support agencies, as well as the means by which to initiate support.
- Discuss the level of support available or desired—as well as what it will cost.
- Confirm whether nonreciprocal or reciprocal agreements (or mutual aid agreements) are preferred, or memorandums of understanding (MOUs) and reciprocal agreements.
- Identify where IMP responses can be augmented or enhanced by the integration of external supporting agencies.
- Identify where security plans can be integrated to further enhance project security.

THE VALUE In foreign, remote, or challenging environments, it is rare that any business operates in complete isolation, whether it is a gold mining operation in Kazakhstan, an oil refinery in Indonesia, a hotel chain in Nigeria, or a textiles plant in India. Establishing good rapport with external agencies can provide some degree of sharing or transfer of risk responsibility. External agencies can give invaluable support in identifying threats through the use of good intelligence as well as providing risk reduction measures. They may also be useful in assisting with incidents and contributing to the positive resolution and closure of incidents. A good example is the link between the civilian police and the military for the security of sensitive locations, with the provision of accurate intelligence, interception of known individuals, area cordoning support, handling of individuals, and any crime scene investigations that may result. Federal agencies can also support efforts against counterfeiting and cyber crimes, coercion and intimidation rackets, and insurgent or terrorist targeting of company interests. Comprehensive joint exercises with agencies that might provide assistance to large, complex or high profile organizations should be included in the risk management program. If necessary, external support representatives should be included on the crisis management team.

In some circumstances company project sites might have an outer security ring of collocated military forces, such as coalition or United Nations military groups or host nation government or tribal security forces. In some areas, there may be no such forces, or they might not be positioned to support project operations and security. At worst, local security may be unreliable or, in extreme cases, complicit in disrupting the project or business venture. Even in the worst cases, however, it is still useful to consider liaison with local security forces for their inclusion into the outer security ring so as to avoid unnecessary polarization of the project. Engagement plans often support an intangible but highly valuable layer of risk management for business activities. The establishment of project operations in the most extreme of environments should consider the incorporation of external support such as military organizations and local security into the project security team, ensuring a layered security footprint with overlapping security arrangements to significantly strengthen project operations, as well as allow the company to more effectively respond to crisis incidents. In these circumstances a clear understandings of the cost against benefits should be established as well as how such integration might bring additional risks to the company. Exhibit 1.27, Crisis Response: Interface Plan, illustrates how the

	Agreement	Armored Vehicle Evacuation	Soft Skin Vehicle Evacuation	Air Evacuation (Regional)	Air Evacuation (National)	Provision of a Safe Haven	Casualty—First-Line Medical Support	Surgery—Medical Support	Armed Quick Reaction Force	Emergency Armed Facility Guards	Explosive Ordnance Clearance Support	Intelligence and Threat Warnings	Legal Support	Mutual Mass Evacuation Plan	Kidnapping and Ransom Advisory Services	Emergency Water Provision	Emergency Food Provision	Emergency Generator Provision	Arrest and Detention Support
Company Y	Written MOU	✓	✓				✓		✓	✓		✓		✓					
Local Militia	Written MOU		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓
U.S. Embassy	Verbal MOU			✓	✓	✓	✓					✓	✓		✓				✓
Coalition Forces	Written MOU	✓		✓		✓	✓	✓	✓		✓	✓				✓			✓
Company X	Verbal MOU		✓			✓						✓		✓					
Security Company Z	Contracted	✓	✓				✓		✓	✓	✓	✓			✓	✓	✓		

EXHIBIT 1.27 Crisis Response: Interface Plan

company can display in a simple way the range of crisis response support it may have available from external groups.

Interface plans in terms of support and resource provisions will be influenced by any difficulties that the groups offering collaborative support to the company might also be experiencing. Occasionally a risk event will affect all parties, at which time those resources offered will be tied to meeting the needs of the owners. Therefore, the interface plan should not be considered the single answer to dealing with crisis events, but rather a multiplier of capability. Interface plans also are designed to indicate what support or agreements are in place, rather than the more granular level of resources actually provided in terms of quantity or frequency—this is an aspect of the *resource management plan*. The two plans should be linked where appropriate as complementary elements of the Business Continuity Management Plan.

LOCAL GOVERNMENT INTERFACE In both passive and hostile environments, it can be useful to liaise with host nation government offices and agencies, in terms of both coordinating security plans and securing emergency support in case of a hostile incident or medical evacuation. In addition, liaison with local law enforcement and military agencies can be useful in the event of an arrest or a detention. Local government and security forces can also offer information on the risk environment and possible calendar events that might affect the company, as well as physical support to the company that might reduce risk. In addition, local government relationships can be leveraged to provide insights into how to work more effectively within a local community, although at times local government groups may be complicit within any threats faced to the company. In many countries, both national and local government officials may be corrupt; in such cases, ways to avoid supporting corrupt or illegal activities while still supporting and engaging leadership, communities, and nationals through employment should be considered as part of an overall business and security approach. The delineation between corruption and local business

customs and practices should also be considered as part of the strategic approach, as these may not always be clear-cut.

LOCAL COMMUNITY INTERFACE The success of projects often depends on local community support, and companies should leverage their own as well as any contracted vendor's local experience, relationships, and knowledge to establish a community liaison and development plan to support their business goals. This is especially relevant in challenging environments where a local community can actively oppose business operations or, conversely, reduce threats through resistance to or the reporting of hostile activities. Community opposition (or support) is frequently found in third-world or postwar environments, such as some African states, where major oil companies encounter significant issues due to poor local relationships, despite considerable local development efforts and social programs. Dealing with the local community requires an understanding of the culture, power brokers, and local influences. A significant degree of sensitivity often is required to avoid misunderstanding or offense, both by the company and by the subcontracted vendors. Successful relations and communication with the local community can be the critical aspect of risk mitigation and incident management for project operations, and corporate and program managers must establish the level of interaction that might be required to support their business needs.

Where possible, local communities and leadership should be included in both the planning and the implementation of all appropriate project activities. During the assessment phase of project planning, various community representatives—ministries, governors, local police forces, elders, religious leaders, and representatives of various associations at provincial, district, and village levels—might be included in planning conferences. It might be useful to interview these stakeholders to identify their thoughts regarding security and project impacts as well as their own community needs and possible socioeconomic or engagement plans. These same individuals and groups should be consulted during the implementation phase of the activity, and regular meetings should be held to sustain strong local relationships. By involving the local community from the outset of a project, a company can gain a level of acceptance, reducing risk and ensuring that external resources can be called upon to support incident management. The following guidelines might be useful in creating a successful relationship with a local community:

- Confirm the company's policy and intention of engagement with the local community.
- Establish an understanding of the local culture, especially sensitivities.
- Identify the *real* power brokers and leaders.
- Establish the best way in which to engage and communicate with local leaders.
- Conduct an intelligence review of local community involvement in possible hostile activities.
- Review possible methods by which to gain trust and support from the local community—investment in schools, medical support, and so forth.
- Consider local leadership meetings to discuss the impact of operations on the local community.
- Involve the community in decision making where possible to gain buy-in.
- Discuss methods by which hostile activities can be reported.

- Consider methods by which to employ the local community, where appropriate.
- Engage local businesses and ventures in partnering or subcontractor arrangements.

EXPATRIATE GOVERNMENT AND DIPLOMATIC INTERFACES Whether a company is operating in Africa or Afghanistan, it is always useful to establish liaison with embassies and foreign forces in order to seek additional support for a business activity's crisis management and incident response requirements. This might be direct relationship development between the company with an embassy, or through working groups organized or supported by governments. At times these external groups will offer little or no support; on other occasions their support may be critical to the success and safety of the project during a crisis event. Any level of international cooperation outside of organic company-contracted resources brings additional knowledge, expertise, and capabilities that would otherwise be absent. An appreciation of the external group's strengths and weaknesses is required in order to ensure that the business activity does not become reliant on inconsistent levels of support. Where possible, memorandums of understanding (MOUs) between the company and government or military forces should be established to define what will, might, and will not be provided to the company.

Also, if the company's activities bring a benefit to a country—whether providing economic development, agricultural programs, or education and employment—embassies may consider a commercial project to be an indirect element of their own programs and goals, and may be persuaded to offer support that otherwise might not be expected. Both the company and the vendor should seek synergies with foreign government interests in order to identify and leverage any value their business may bring to that government. Companies should also research government support agencies and resources in order to ensure that they understand what is available to them—what capabilities and resources they can leverage and where they can draw upon proven experience and materials to design or enhance existing policies, plans, and approaches.

Some government agencies will support businesses operating both domestically and abroad, offering advice and practical support to enable better business preparedness and recovery. Exhibit 1.28 provides examples of such organizations.

OTHER COMPANY INTERFACES Companies should consider establishing reciprocal or mutual aid agreements with other commercial organizations to establish and leverage a consortium of support. Such organizations as the Overseas Security Advisory Council (OSAC) and Security Information Service for Business Overseas (SISBO) set up forums to centralize issues and solutions for U.S. and UK businesses and organizations abroad, and the company may wish to exploit this concept by drawing strength from other commercial groups. It might be possible and appropriate (with permissions from the company and the vendor) for the company to develop reciprocal arrangements with other commercial organizations to augment security policies, procedures, and responses. Mindful of commercial and liability risks, companies can mitigate threats with measured integration of specified fields and areas with external organizations, through either loose or formal agreements. In addition, and perhaps more importantly, responses can be greatly enhanced if companies provide mutual

EXHIBIT 1.28 Supporting Organizations for Business Continuity Management Interface Plans

Organization	Web Site	Remarks
Overseas Security Advisory Council (OSAC)	www.osac.gov	U.S. government–based organization designed to support U.S. businesses overseas in terms of advisory councils and security education
London Resilience Forum	www.londonprepared.gov.uk	UK government–based organization focused on business risk management for companies operating within the London area (United Kingdom)
Security Information Service for Business Overseas (SISBO)	www.fco.gov.uk/en/business-trade/sisbo/	UK foreign and Commonwealth office designed to advise British businesses overseas on security and risk management issues
Federal Emergency Management Agency (FEMA)	www.fema.gov.com	U.S. federal disaster and emergency response organization
National Response Framework (NRF)	www.fema.gov/emergency/nrf/	Division of FEMA responsible for supporting unified responses to crisis events, as well as for organizations preparing business continuity, management protocols and plans
Department of Homeland Security	www.dhs.gov	U.S. government agency providing advice to individuals and businesses on security related issues, as well as crisis response
Locating an Emergency Agency	www.rateitall.com	Provides guidance on different emergency and disaster response organizations
Washington Military Department: Emergency Management Division	www.emd.wa.gov	State government organization focused on military cooperation for crisis response in the state of Washington
Northeast Document Conservation Center (NEDCC)	www.dplan.org/	Provides a free disaster planning tool to help organizations evaluate and manage risk

cooperative agreements where other company facilities and resources can be used by a threatened group during time of need.

Medical Response and Repatriation Plan

Often local managers will be required to deal with a range of medical emergencies—from heatstroke for site workers to falls, breaks, heart attacks, and general illnesses. A medical emergency within a domestic setting where emergency services can respond quickly and administer medical stabilization en route to more comprehensive facilities can test an organization and first responders; add to this a remote site, hostile environment, or third-world transportation mediums and medical facilities,

and the crisis can become even more pronounced. At worst, companies may have to deal with a life-threatening condition that requires immediate stabilization and evacuation to distant medical facilities, or in some instances the repatriation of a fatality to the home country from a foreign work area.

Companies should develop a medical response and repatriation plan in order to manage various situations, from the common daily and mundane problems to the unique and significant medical emergencies that would face any workforce, and place this plan in the context of the operating environment in which personnel are working. For medical emergencies, companies should consider the basic elements of:

- Stabilization and initial treatment of casualties.
- Movement in-country to secondary care facilities (multiple movement mediums).
- Comprehensive (surgical and specialist) treatment facilities.
- Movement from country to Western clinics and hospitals out of country.
- Insurance coverage and payment plans.
- Safe and secure treatment considerations.

For repatriations of remains, companies should consider the following basic elements for the effective movement of a deceased employee from the country:

- Cold storage and container resources for cold storage.
- Movement in-country and transfer points for cadaver storage.
- Documentation requirements and insurance stipulations.
- Autopsy and embalming requirements and providers.
- Air freight and escort resources and policy guidelines.
- Family liaison and support services.
- Reporting and documentation needs.
- Morale and welfare implications for staff.

Companies should have clear and well-planned measures in place to deal with medical emergencies, as well as the first stages of a repatriation task. The IMP will play a key role in the initial response to both requirements, ensuring that resources are mobilized to quickly move a casualty through a medical evacuation process, or ensure that a fatality is properly administered from the outset. The medical response and repatriation plan may be linked to a section within the interface and resource management plans in terms of drawing upon or leveraging organic and external support, as well as defining which resources will support medical and repatriation tasks.

Public Relations Plan

Crisis events will invariably affect the image and reputation of a company, at times attracting hostile attention from the media or special interest groups. The company's reputation is an intangible commodity whose value has serious and at times devastating consequences to a company if undermined. The ease of broadcasting information or images worldwide and through multiple mediums can create an immediate and catastrophic crisis for companies as they struggle to establish facts and control over an event themselves, often resulting in companies lagging behind the media in terms of understanding and responding to a crisis situation. The value of the IMP in terms

of separating facts from rumor or speculation, as well as exerting control over the event, is an important contributing element of a public relations plan.

Corporate or crisis communications through a public relations medium is designed to safeguard the value and confidence of a company's brand, as well as the image and reputation of a company, group, or business activity. Reputation might be defined as the social or commercial evaluation toward a person, group, or organization. It is especially important to businesses whose stock values and market productivity are directly connected to their status within a commercial sector and dependent on investor and client confidence. Mature public relations plans can also offset the effects of liability claims and publicly demonstrate the company's efforts to mitigate risk and protect employees, investments, or activities. Public relations might be focused outward, meeting external risks to the corporate interests, as well as inward, protecting the morale and productivity of the employees.

Reputation acts on different levels of agency—individual and supra-individual. At the supra-individual level, reputation concerns groups, communities, collectives, and social entities such as firms, corporations, organizations, countries, and cultures. It affects phenomena of different scale, from everyday life to relationships between nations. The impact of reputation is often ignored, with no clear or tangible connection toward associated *real* impacts upon business success and operations. Reputation includes *image*, a global or averaged evaluation of a company—its activities, productivity, capabilities, and executive management competence. Reputation often aligns with the perceived image or branding of a business. Image is a dynamic element and subject to immediate change, either through actual events or through speculation and rumor. Misinformation or erroneous reporting can severally damage a company's image and thus reputation, and reputation recovery is often difficult, problematic, slow, and highly costly. Therefore, a defining value of the IMP is supporting accurate reporting from the outset of a crisis.

Companies such as Johnson & Johnson, as well as more recently CACI International Inc., have invested millions of dollars in protecting their brands and corporate interests resulting from such incidents as the Tylenol poisonings and the Abu Ghraib prison scandal. Companies should understand their strengths as well as limitations and seek outside support where necessary to ensure they have a robust public relations plan. Developing a plan that is aligned to strategic and granular risks can better position the company to manage reputational and liability risks resulting from a crisis situation.

PUBLIC RELATIONS DEPARTMENTS Establishing a well-trained public relations department to deal with media and general public inquiries is necessary to ensure that an organization reduces potentially harmful press coverage during normal operations, but especially in the event of an emergency situation. The establishment of an effective communications plan, media management measures, and accurate reporting measures, or a crisis communications system, ensures that the collation of information is swift and accurate, with an efficient and sanctioned means of delivery to the relevant elements of a crisis management team, employees, their families, often antagonistic news media, and other relevant agencies in a timely and accurate manner. The IMP plays a key part in developing early information reporting flows and supporting the public relations department in defining the company's stance

and approach to an event—as well as the facts of the situation. Some corporate and public image aspects to contingency planning include:

- Providing only proven facts—avoid speculation or assumption.
- Understand the situation as quickly as possible—investigate immediately.
- Demonstrate that focus is being applied and resources mobilized.
- Be honest and up-front—admit blame but challenge erroneous reporting.
- Respond to inquiries and robustly question errors.
- Consider multiple communications mediums to get the message across—interviews, conferences, web sites, publications, announcements, television, and radio.
- Vet information and sanction release.
- Have a well-trained and experienced spokesperson—ensure that the spokesperson has all the facts.

Companies should establish an effective intermediate body between the management executive and external agencies (media, families, government) to ensure that the corporate image is promoted and maintained, while avoiding unnecessary speculation and inaccurate allocation of blame by the media or general public. Erroneous speculation often leads to a loss of confidence within an organization and undermines the aims and values of the group. A company may wish to provide training as well as preprepared public announcements to respond to likely threats, thus ensuring that staff are readied, with supporting materials, to deal with an incident quickly and effectively.

ESTABLISHING THE FACTS The IMP will play a critical part in allowing corporate leadership to implement an effective public relations plan during the early stages of a crisis event. Accurate and timely reporting of information allows the public relations officer to determine the company risks, their impacts, and the appropriate stance the company should take to best manage the situation. The data call reports within the IMP, sent typically from the point of crisis, will guide decision making as more senior and experienced resources are mobilized to manage the issue and consolidate the flow of information within the group. The public relations plan might therefore have stages—the immediate responses to meet initial questions from media groups, as well as more mature and measured response stages to manage longer-term issues.

Information should always be accurate and factual; speculation should be avoided. Information should be verified to ensure accuracy, and where possible transparency should be adopted as a guiding principle, as this often meets the longer-term interests of a company. Companies should avoid rushing to judgment until all the facts are known and verified.

PRESENTING INFORMATION Only trained and experienced spokespeople should interact with the media and other groups in order to protect the company's interests. Information should be vetted through corporate officers, as well as legal resources if appropriate, prior to release. Often prepreparing press releases to meet postulated public relations crisis events can support the company in delivering information in a more measured and professional manner, rather than wasting valuable time

EXHIBIT 1.29 Sample Preprepared Press Release

An industrial accident occurred at _____ resulting in ___ fatalities and ____ injuries. The cause of the accident resulted from _____. The situation at the site is now under control and we have activated our crisis response measures in partnership with the emergency response services in order to ensure the safety of the workers who have remained on-site. There is no danger to residents within the area; however, we would ask you to stay away from the site so that access routes are not blocked and the emergency services can do their work. As you can appreciate, we are working hard to gather all the facts while we manage this crisis situation, so that families can be contacted as quickly as possible and advised of the situation and the welfare of their loved ones. We would ask the media to respect and be sensitive to the losses and concerns of the workers' families at this time, avoiding speculation and rumor. We have established an emergency hotline, and families can speak to our crisis management team on _____. We will also be providing regular verbal updates at our crisis center located at _____. We will hold briefings every ____ hours, starting from _____. We will ensure that accurate information is passed on to families and the media as quickly as possible. Please be patient at this time. We will provide the next update at _____. We will also post information on _____.

during high-stress and fast-tempo crisis management situations. Such preprepared press releases might follow the simple format in Exhibit 1.29.

Such preprepared press releases can cover a broad spectrum of likely events and support timely and well-crafted public information releases to demonstrate that the company has some degree of control over the situation and is attempting to meet the needs of both families and the press concurrently. Such releases may reduce the level of speculation and might be fed from IMP data call report information.

Resource and Procurement Management Plans

The Business Continuity Management Plan will function well only if properly resourced. In terms of contingency planning, resource scheduling and cross-utilizations should be components of the overall service delivery goals of both the company and any subcontractors. In terms of implementing both the IMP and more comprehensive and subsequent crisis plans, resource management can be a critical component in effectively managing a catastrophic situation. Many aspects of crisis response will be dependent upon the availability of resources, whether they are buses to move evacuees to an extraction point, food and water to sustain those caught within a disaster area, or fiscal provisions to mobilize external support agencies. Resourcing can be considered in terms of:

- Corporate buy-in and senior-level support for the concept.
- Understanding and acceptance at all levels across the organization.
- Clear and known permissions, decision authorities, and operating parameters.
- Design and development of policies and procedures.
- Training and education to support policies and procedures.
- Technological infrastructure and materials to utilize plans.
- Communications infrastructure to enable information flow.
- Physical structures, materials, and resources to support the plans.

- Appropriate managers and personnel to implement policies and responses.
- Predeployment materials and resources to support responses.
- Contracted support for external advisers or specialists.
- Leveraged government or other group plans and agreements.
- Scheduling and cross-utilization policies and systems.

RESOURCE MANAGEMENT PLAN The Business Continuity Management Plan should contain crisis resource and procurement management plans in order to identify what resources might be required, where gaps may lie, and how organic and outsourced resources can be utilized, in strategic or conceptual terms, as well as practically. Exhibit 1.30, Crisis Response: Resource Management Plan, illustrates some tactical-level resource plan components.

The resource management plan might contain owned company resources spread across multiple project sites, as well as those resources that might be leveraged, either through collaborative agreements with other organizations or procured from commercial sources as required. At the corporate level, the resource management plan might contain teams within the company crisis response team, as well as outsourced support, including aviation companies, stress trauma adviser, legal support, medical services and public relations consultants.

There is also value in determining what the resources mean in terms of implementing the crisis response measures. For example, if the project site has 32 staff members and only three armored vehicles capable of transporting five people each, a maximum of 15 personnel may be moved in each motorcade lift. Only materials crucial for the crisis response plans should be included—for example, water resources in arid climates, weapons in hostile environments, or vehicles and fuel storage in remote project sites. Resource plans may also contain sections covering services in terms of medical support, transportation resources, and repatriation assistance. The resource plan should lay out materials, services, and advisory or

Organic Resources	Armored Vehicles	Soft Skin Vehicles	Passenger Buses	Safe Haven Capacity	Medical Packs	Assault Rifles	Pistols	Night Vision Goggles
▪ Project Alfa	3	4	1	43	2	12	2	1
▪ Project Bravo	6	5	3	22	4	8	6	1
▪ Project Charlie	9	8	2	12	8	8	3	2
▪ Project Delta	2	7	4	56	2	8	2	0
▪ Country Center	4	7	1	98	6	22	12	2
Total Resources	**24**	**31**	**11**	**231**	**22**	**58**	**25**	**6**
▪ Required Resource Level	32	12	13	332	4	65	22	3
▪ Combined Resources	64	60	14	653	26	58	25	6
▪ Organic Capability Variables	8	–19	2	101	–18	7	–3	–3
▪ Final Variable Evaluation	32	48	1	321	22	–7	3	3

External Resources	Armored Vehicles	Soft Skin Vehicles	Passenger Buses	Safe Haven Capacity	Medical Packs	Assault Rifles	Pistols	Night Vision Goggles
▪ 12th Battalion—ISAF	34	4	2	320	0	0	0	0
▪ Company Y	2	12	0	34	2	0	0	0
▪ Company X	4	1	1	23	0	0	0	0
▪ Company C	0	12	0	45	2	0	0	0
Total Resources	**40**	**29**	**3**	**422**	**4**	**0**	**0**	**0**
▪ Required Resource Level	32	12	13	332	4	65	22	3
▪ External Support Variables	8	17	–10	90	0	–65	–22	–3

EXHIBIT 1.30 Crisis Response: Resource Management Plan

facilitatory arrangements both in-house and through leveraged or contracted agencies. This may also be linked to the procurement plan if monies need to be expended to mobilize external support for crisis response needs.

The resource management plan should consider compatibility for interfaced resources to ensure that resources can work to support each other; this is especially relevant if the IMP relies on specified support agencies that might use different consumable materials or technological features for the same resource item, whether it is short ammunition for long ammunition rifles, gasoline compared to diesel fuels for vehicles, or frequencies for radios. Exhibit 1.31 illustrates a simple resource integration chart that might be useful for companies when leveraging external group capabilities and materials. This can be used to indicate where support may be leveraged, as well as shortfalls in quantity and quality, in addition to other problems or compatibility failure points. Resource plans should generally be held within the Business Continuity Management Plan, unless specific elements relate directly to IMP activities or responsibilities. Resourcing should also be considered in terms of prepositioning equipment or resources that response teams might require. These might include food and water, tools, medical supplies, transportation and fuels, ammunition, communications technology, and temporary shelter.

CRITICAL MATERIALS REGISTER The company should develop a critical materials register to ensure that all high-value, sensitive, or strategic materials and information are identified as part of the risk evaluation and preparedness planning aspect of the Business Continuity Management Plan. The register might include:

- Materials, equipment, and information that are critical for operational success.
- Materials that are irreplaceable or of significant monetary or reputational value.
- Materials that if lost will place the company at liability or legal risk.
- Materials that could present harm if acquired by unauthorized persons or groups.

The Business Continuity Management Plan should identify those items that are deemed critical to the company and evaluate the probability of a risk occurring, as well as the implications should the threat materialize, as illustrated in Exhibit 1.32, Critical Materials Risk Evaluation Matrix.

The company will be best placed to determine which materials will be considered part of a critical materials register from a corporate perspective; however, it should also ensure that materials that would be included as part of external value considerations—governments, industry counterparts, and so on—are listed as well where appropriate. Such materials might include:

- Radioactive materials or toxic chemicals.
- Weapons, explosives, and ammunition.
- Critical machinery, technology, or materials.
- Government-restricted items: encrypted radios, night vision technology, information technology (IT).

Relevant components of the Business Continuity Management Plan, as well as its constituent elements, should be aligned to managing the risks presented by the loss or damage to such materials. Specific response plans may also be developed to

Company Agency	Required Resource Type	Quantity	Amount	Frequency	Compatible	Quantity	Available Resource Type	Support Agency
Project Delta	Diesel Fuels	500ltrs	Neg100ltrs	Monthly	No	400ltrs	Petrol Fuels	3rd Armor Bde
Project Delta	7.62mm Ammo (long)	36,000rds	Neg10,000rds	Semiannually	No	26,000rds	7.62mm Ammo (short)	4th Armor Bde
Project Delta	Handheld Radio Type	Motorola	NA	1284.8686	No	Military	Handheld Radio Type	5th Armor Bde
Project Delta	CCTV Systems	Delta	NA	768696.0	Yes	Military	CCTV Systems	6th Armor Bde
Project Delta	VHF - Freq. 1.26363	NA	NA	NA	Yes	NA	VHF - Freq. 1.26363	Company X
Project Delta	Diesel Fuels	10,000ltrs	✓	Weekly	Yes	10,000ltrs	Diesel Fuels	4th Armor Bde
Project Delta	24-Man Tentage	4	✓	Once	Yes	4	24-Man Tentage	4th Armor Bde
Project Kilo	Diesel Fuels	20,000ltrs	Neg2,000ltrs	Weekly	No	18,000ltrs	Petrol Fuels	3rd Infantry Bde
Project Kilo	7.62mm Ammo (long)	24,000rds	Plus4,000rds	Semiannually	No	28,000rds	7.62mm Ammo (short)	Company A
Project Kilo	VHF - Freq. 2.26363	NA	NA	NA	No	NA	VHF - Freq. 1.26363	Company C
Project Kilo	Handheld Radio Type	Motorola	NA	1284.8686	No	Military	Handheld Radio Type	4th Armor Bde
Project Kilo	Diesel Fuels	3,000ltrs	✓	Monthly	Yes	3,000ltrs	Diesel Fuels	5th Armor Bde
Project Kilo	24-Man Tentage	17	Neg1	Once	Yes	16	24-Man Tentage	Company A
Project Kilo	Portable Water	2,000gals	Neg500gals	Daily	No	1,500gals	Gray Water	Company A
Project Xray	5.56mm Ammo (NATO)	15,000rds	✓	Semiannually	Risk	15,000rds	5.56mm Ammo (Russian)	Group C
Project Xray	VHF - Freq. 2.26363	NA	NA	NA	No	NA	VHF - Freq. 1.26363	3rd Infantry Bde
Project Xray	Diesel Fuels	9,000ltrs	Plus1,000ltrs	Weekly	Yes	10,000ltrs	Diesel Fuels	Company A
Project Xray	24-Man Tentage	6	Plus2	Semiannually	Problem	8	16-Man Tentage	Embassy C
Project Xray	Portable Water	10,000gals	Neg1,000gals	Daily	Yes	9,000gals	Portable Water	Company D

EXHIBIT 1.31 Resource Compatibility Table

Critical Material	Probability of Loss	Impact Level	Project 1	Project 2	Project 3	Project 4	Project 5	Project 6
IT Server ■	3	E	✓	✓	✓			
Well Rig Unit ■	3	E	✓	✓				
Minatron Source ■	1	E	✓	✓	✓	✓	✓	✓
Industrial Explosives ■	1	M		✓				✓
Encrypted Radios ■	3	H	✓	✓	✓	✓		
Coiled Tubing Unit Rig ■	3	H			✓	✓	✓	
Night Vision Technology ■	3	M		✓		✓		
Weapons ■	1	H	✓		✓	✓	✓	
Ammunition ■	2	M				✓		✓
Toxic Chemicals ■	1	H	✓	✓		✓	✓	✓

Probability Levels	Impact Level
1 - Highly Unlikely to Occur	**N**egligible
2 - Unlikely to Occur	**L**ow
3 - Possibility of Occurrence	**M**edium
4 - Likely to Occur	**H**igh
5 - Expected to Occur	**E**xtreme

EXHIBIT 1.32 Critical Materials Risk Evaluation Matrix

manage both immediate response actions (the IMP) and more comprehensive and complex response measures.

PROCUREMENT PLAN Resource management policies and procedures should be components of crisis resource and procurement management plans, where management teams can most effectively understand what organic capacity the company has, both on-site and in terms of emergency resource reallocations, as well as where external agencies and vendors can be leveraged or contracted to meet resource or capability gaps.

The company will have a finite amount of in-house resources and capabilities, which is typically aligned to meet normal operating requirements. A margin may have also been factored into the project in order to meet surge requirements, or certain emergency situations—although often this additional cost is unacceptable for most groups and the "buy as you need" approach is adopted. Even when other project or supporting agencies' resources are fully brought to bear, resource gaps may still remain that must be met through commercial vendors or other supporting groups—typically at a significant cost. A useful aspect of the contingency component of the Business Continuity Management Plan is a procurement plan, providing permissions and parameters for staged procurement activities to meet immediate, interim, and long-term resource procurement needs. In order to streamline procurements, it is useful to limit the number of managers who are authorized to sanction procurements. This avoids duplication and better defines responsibilities.

It is also useful to have established some form of price estimate or basic ordering agreement with service providers prior to a crisis event in order to define

Corporate—Strategic	Stress Trauma Consultancy	Charter Airline Services	Repatriation Services	Reception Facilities	Maritime Resource Services	Medical Services	Legal Counsel	Kidnap and Ransom Consultancy
Corporate Crisis Manager	✓	✓	✓	✓	✓			✓
Corporate Security Director	✓				✓	✓		
Administration Manager		✓	✓	✓				
Human Resource Director	✓						✓	

Project—Tactical	Personal Security Details (PSD)	Facility Guard Services	Local Medical Services	Rotary-Wing Air Services	Land Transportation Leasing	Life Support Stores	Ammunition and Defense Stores
Country Crisis Manager			✓	✓	✓	✓	
Country Security Manager	✓	✓					✓
Program Crisis Manager					✓	✓	
Project Crisis Manager					✓	✓	

EXHIBIT 1.33 Crisis Response: Procurement Plan

the operational constraints of a service, as well as the cost implications. This can be problematic and is hard to justify if a cost is attached, however, this approach will enable outsourced services to be mobilized more quickly without placing the company at financial or operational risk. Exhibit 1.33 illustrates a simple layered procurement plan, ranging from corporately driven strategic and high-value leases and purchases to more tactical field-level procurements.

Project Initiation Plans

Integral to the Business Continuity Management Plan should be procedures, protocols, and policies for starting (or expanding) business activities within new regions. It is typically when entering a new market or geographic area with which the company is not familiar that the greatest risk exposures may occur. Managers at both corporate and program levels will be seeking to understand the new and unfamiliar operating environment, and new policies and plans will need to be created, or existing ones modified, to reflect nuances connected to cultural, geographic, or climatic influences. Establishing a comprehensive framework document, which follows a systematic and logical approach to ensuring that project requirements are planned within a risk and security context, is critical for companies seeking to operate in new, remote, or challenging environments. By adopting a system such as the one illustrated in Exhibit 1.34, companies are better positioned to ensure that strategic as well as operational and tactical requirements are met in full. This approach should be adopted throughout the business and project planning cycle—addressing each planning and management stage of business justification, proposal development, project design and planning, project initiation, and work package delivery and sustainment—until closure of each work package, as well as the overall program.

Exhibit 1.35 details how each component will support the development of comprehensive and pragmatic policies and plans for companies seeking to operate within new operating areas.

A systematic and logical approach to planning should be employed so that strategic, operational, and tactical requirements are met in full, avoiding errors or

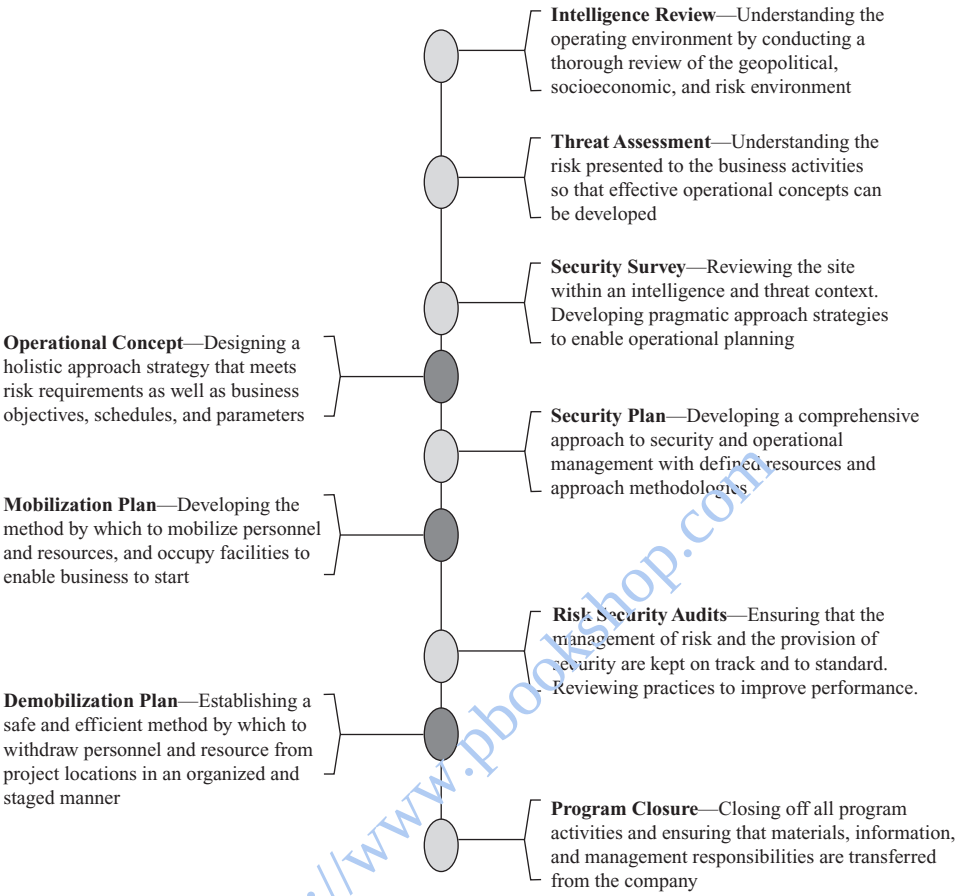

EXHIBIT 1.34 Project Initiation Document Development Sequence

gaps within the planning process that could undermine business goals, productivity, and bottom-line profits, as well as expose personnel, materials, or the company to unnecessary risks.

Business Recovery Plans

Effective business resilience measures will enable companies to better weather a crisis and continue to be productive during an event. However, in some instances business will be forced to stop and personnel and resources may go through a period of stasis, or may even be withdrawn from task until the situation stabilizes. It is in the interests of the company to determine when work can begin again, within permissible risk tolerance parameters, through a staged and predefined business recovery plan. Business recovery planning may involve corporate decision making in terms of the business risks of continuing operations, or the long-term political or liability risks associated with an event that may have initially disrupted operations. The damage to infrastructures and utilities resulting from a natural disaster may also

EXHIBIT 1.35 A Logical Sequence for Designing Policies and Plans

Strategic Stage	Description	Strategic Process	Outputs
• **Intelligence Review(s)**	Understanding the operating environment by conducting a thorough review of the geopolitical, socioeconomic, and risk environment.	Conduct intelligence reviews through open and closed sources to deliver specific information reports—enabling intelligence led management planning processes.	■ Populace Intelligence Reports ■ Threat Assessment Intelligence ■ Strategic Political Reviews ■ Key Groups and Leadership Reports ■ Risk Register ■ Risk and Impact Mapping ■ Threat and Impact Matrices ■ Strategic Mitigation Strategies ■ Detailed Security Assessments ■ Policy and Plan Data Collection ■ Answers to Corporate/Program Questions ■ Formulation of Practical Approach Needs ■ Overarching Policies and Procedures ■ Defined Resource Requirement Plan ■ Defined Action Plan, with Costs ■ Aligned Risk and Project Gantt Charts ■ Interface, Leveraging, and Outreach Plans ■ Facility Security Policies and Plans ■ Associated Evacuation Plans ■ Associated Incident Management Plans ■ Associated Interface and Leveraging Plans, as Well as SOPs and TTPs ■ Developing an Operations Order ■ Designing a Resource Leveraging Plan ■ Identifying an Advance Team ■ Identifying Long Lead Procurements ■ Hardening Facilities and Structures
• **Threat Assessment(s)**	Understand the risk presented to the business activities so that effective operational concepts can be developed in alignment with corporate needs.	Place the intelligence information and business requirements into a detailed threat context, mapping risks and impacts through each stage of the program.	
• **Security Survey(s)**	Review the site within an intelligence and threat context—developing pragmatic approach strategies to enable operational planning.	Undertake remote and field security surveys of operating areas and project sites in order to scope the practical requirements and define risk in practical terms.	
• **Operational Concept**	Design a holistic approach strategy that meets risk requirements as well as business objectives, schedules, and parameters.	Design an overall operational approach to delivering services through various work stages within the program, bringing together risk and security management issues and program goals, schedules, and objectives.	
• **Security Plan(s)**	Develop a comprehensive approach to security and operational management—with defined resources and approach methodologies.	Build the operational policies and plans for specific static and mobile operations, defining methods of operation, risk mitigations, and resource development and usage approaches.	

(*continued*)

EXHIBIT 1.35 A Logical Sequence for Designing Policies and Plans (*Continued*)

Strategic Stage	Description	Strategic Process	Outputs
• **Mobilization Plan(s)**	Develop the method by which to safely and effectively mobilize personnel and resources, and occupy facilities to enable business to start.	Build a Project Initiation Document in order to define resource procurement, development, and deployment in alignment with program schedules and goals.	■ Risk and Security Policy Audits ■ Risk and Security Operational Audits ■ Training and Development Audits ■ Asset Management Audits ■ Financial Management Audits
• **Risk and Security Audit(s)**	Ensure that the management of risk and the provision of security are kept on track and to standard. Review practices to improve performance.	Conduct clinical and impartial reviews of performance and management in order to manage quality, and evidence corporate governance throughout the life span of the program.	
• **Demobilization Plan(s)**	Establish a safe and efficient method by which to withdraw personnel and resources from project locations in an organized and staged manner.	Develop a safe and effective policy and plan to withdraw personnel and materials from project sites, or to close down the program.	
• **Program Closure**	Close off all program activities and ensure that materials, information, and management responsibilities are transferred from the company.	Collect and collate information, materials, reports, documents, and materials for storage within effective files, documents, and reports.	■ End of Project Reports ■ End of Program Reports ■ Transition or Relief in Place Plans ■ Administrative Closure Reports

undermine the business rationale to continue operations. On an operational level, business recovery may be focused on two main areas:

1. **Reoccupation Recovery.** The point at which offices, work sites, accommodations, or facilities are reoccupied following an evacuation by some or all of the project staff.
2. **Business Recovery.** The point at which workers return, movement starts, meetings occur, facilities open, and operations resume, enabling staged business to restart.

REOCCUPATION RECOVERY The evacuation of a site, facility, office, or in some cases country may be only temporary, leading to the staged return of people and materials to the project site, a situation that enables business to recover and continue after a delay. Companies should consider recovery or reoccupation plans that will enable business activities to start again in a preplanned, logical, systematic, and safe manner. The evacuation may have resulted from man-made problems or a natural disaster, and the implications of the cause of the evacuation should be carefully considered in each instance. Reoccupation of project sites and a restart of operations should be seen almost as a limited version of a mobilization plan, and there are additional factors to consider in terms of heightened security measures, as well as the likely implications of damage and looting that might have resulted following the withdrawal.

Heightened local tensions and government responses may have also changed the threat picture, and floods or other natural disasters may have undermined the rule of law and created additional security instabilities or health hazards that compound the effects of the initial crisis event. The circumstances that led to the evacuation may have made the region temporarily more volatile or, conversely, safer due to the increased presence of security forces. A simple reoccupation planning process is illustrated in Exhibit 1.36, which demonstrates a simple decision and activity path to enable the safe and productive return to work.

When the risk environment has stabilized following the evacuation of a remote site or a region as a whole, a detailed intelligence and risk assessment should be conducted to determine the known and possible new threats facing a possible reoccupation. These threat considerations should not only focus on physical threats, hostile groups, and criminal elements but should also consider disease, logistics resupply, and other more mundane factors. Contingency plans should be reviewed and modified to reflect the changes to the operating environment as part of a return planning process. The company should have already identified an advance team whose responsibilities are to liaise with local leaders or embassy officials in order to gauge the viability of return and to deploy with appropriate security support to review the associated needs for reoccupation, including reviewing the project site itself. The advance team should draft or consolidate an existing reoccupation schedule and plan, as well as project work plans so that a measured return with appropriate lead groups is achieved. This should be a collaborative effort between risk managers and business or project managers. The reoccupation goals are for a safe and productive return of project staff, and it is important that productive business activities can start as soon as personnel and resources arrive on-site. Resources sitting idle at the project site cause the company to incur unnecessary costs and expose

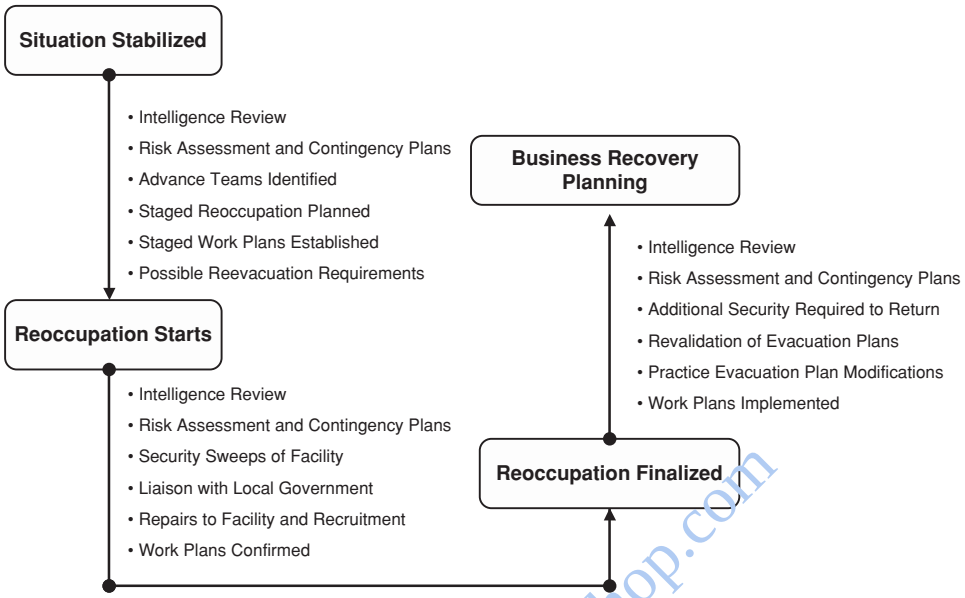

EXHIBIT 1.36 Reoccupation Planning Process

personnel to unnecessary risks. Personnel should deploy only when they can do so safely and when they can operate. The company may wish to define occupation safety levels, such as:

- **Level 1:** Only security personnel are permitted at the location; no company staff members are permitted on-site.
- **Level 2:** Only security personnel and critical project managers are permitted at the location.
- **Level 3:** Security personnel, critical managers, and key project staff are permitted at the location.
- **Level 4:** Security personnel, critical managers, key staff, and normal workforces are permitted at the location.
- **Level 5:** All personnel, including corporate leadership, are permitted at the location.

During the entire planning process, reevacuation considerations should be at the forefront of planning. When reoccupation begins, a continued process of intelligence and risk reviews should be conducted. The facility should be swept for any harmful materials that may have been planted by hostile groups or left by natural hazards. A registry of damages and materials thefts should also be established to ascertain information or material loss that might affect the business goals or the security or safety of the site and activity. Ideally a destruction plan will have been implemented as part of the IMP, meaning that little valuable information or equipment was left behind. Liaison with external groups should be conducted as part of the overall reoccupation process. Needed repairs to the facility and material requirements should be identified and the supply chain system mobilized. Recruitment of local labor forces,

including security personnel, may be problematic following an evacuation, as locals may have been involved in or affected by the cause of the withdrawal. Time may have to be spent reestablishing communications and reenlisting local labor forces.

Project work plans should also be considered to determine which project staff should return and in what order, to avoid unnecessary exposure to risk and to ensure productive business activities. The staged return of project personnel is likely to require additional security resources, in terms of movement and possibly heightened security at the facility while reoccupation occurs. All plans should be revalidated to ensure they are consistent with any changes to the risk environment following the evacuation, and continued liaison and threat reviews should be conducted. The security posture should be more robust immediately following a return, as tensions or problems in the area will likely remain. In many cases the reoccupation presents more challenges and risks than the initial occupation of the site.

BUSINESS RECOVERY Business recovery planning usually presents fewer challenges than a reoccupation recovery, as typically it will form an aspect of such a plan. Business recovery typically occurs when business operations have been forced to be reduced, or stopped, due to natural hazards or due to heightened man-made risks—whether the arrest and detention of personnel, increases in crime, increases in insurgency or terrorist activities, or specific targeting or attacks—causing workforces to be absent, movement to stop, and facilities to close. Business recovery is the staged and logical evaluation of what activities can restart and in what sequence. Exhibit 1.37 illustrates a simple process of returning the company to work, following

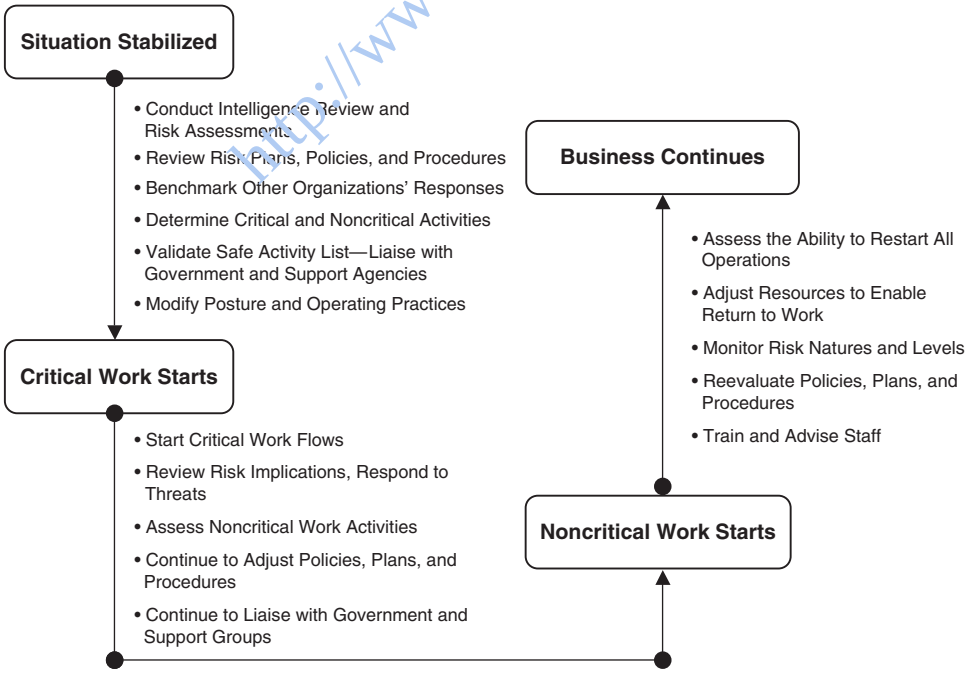

EXHIBIT 1.37 Business Recovery Planning Process

a logical and staged approach. The goal is to evaluate what activities can be conducted safely and in accordance to their order of priority to the company.

Companies should also consider the following key factors as part of their business recovery plans:

- When can local workforces safely return to facilities?
- When can foreign workers safely travel, or return to work sites?
- When can facilities reopen for business?
- What adjustments should be made to operational and risk management approaches?
- What policy changes are required to reflect changes to the risk environment?
- What are the most critical requirements—can they be started first?

Companies should evaluate all factors pertaining to the return to work, whether they be the risk implications of a route traveled by expatriate workers, threats posed to a village from which local workers are sourced, possible profile risks presented by starting business before other similar companies, and the emergency response needs should threats return at any stage of the recovery process.

Postincident Reviews

Following any crisis, the company's management elements should conduct a detailed debriefing at all levels to ensure that all mitigating measures were fully implemented and that any follow-on requirements are actioned. The postincident review should define what went right and what went wrong in terms of the contingency plan, crisis response protocols (including the IMP), and how management structures and decision makers performed. The aim of the postincident review is to address gaps or shortfalls in order that future crisis situations may be better managed. Any supporting security studies, reviews, surveys, threat assessments, or other materials should be clearly stored for internal review as well as external audit. Management should be aware that audits can occur several months or years after the incident. Typically the following auditing activities will occur following an incident:

- **Review the risk assessment.** Did it identify the risks and grade them appropriately?
- **Review mitigation measures.** Did they adequately offset the risks?
- **Review policies and procedures.** Were they detailed enough—did they meet the need?
- **Review management.** Were managers properly prepared—did they apply the contingency plans?
- **Review the vendor.** Did the vendor provide the correct services—did it support crisis management?
- **Review intelligence and risk data.** Are the risks still present—is the crisis over?
- **Strategic planning.** What needs to be done in the immediate, interim, and long term?
- **Deescalating posture.** Can security postures be reduced—if so, when and where?

- **Reviews and audits.** What further reviews and audits are required—when, and from whom?
- **Adjustment.** What approaches, training, policies, and plans need to be adjusted?

The postincident review for significant incidents should be managed by those not directly involved in the event in order to establish an impartial review, although input and participation from the various groups that managed the crisis is, of course, required. Often, utilizing external auditing groups enables corporations to demonstrate, both internally and externally, that they reviewed the incident in a nonsubjective manner.

Summary

The contingency planning measures within the Business Continuity Management Plan should reflect the threats presented within any risk assessments conducted by the company, matching each risk against an avoidance or mitigation approach, including the responses provided with the IMP. Contingency planning measures may be engineered to meet requirements at different levels, meeting corporate, country, program, and project needs. The structuring of the plan should be done in a manner that ensures that tiered policies and responses be met, and that any interaction between different levels of management within the company is understood, as well as with external groups. Contingency measures must reflect dynamic risk environments and should be modified to suit shifting circumstances and needs. The needs and operating methodologies of the business activity will also influence contingency measures, and documents should be written in such a manner as to permit efficient changes without undue effort. The use of tables and stand-alone guidance and policies sections for each risk area will facilitate this, although integration points should be identified so that the final policies and procedures demonstrate an integrated approach. Some data will also be migrated around the plan, and these should be identified and managed to ensure consistency and reduce effort and duplications. Some examples of successful utilization of the Business Continuity Management Plan include:

- **Strategic.** Johnson & Johnson recovered its brand image following the 1982 Tylenol poisonings through effective business recovery measures.
- **Operational.** Using a strategy of supply chain resilience, Wal-Mart was able to bring 70 percent of its stores in the Katrina-affected area back into operation within 48 hours of the disaster.
- **Tactical.** A major (unnamed) oil services company conducted an immediate evacuation of over 120 civilian engineers and workers from one of the most hostile project environments (northern Iraq) due to an industrial hazard.

Where considerable amounts of risk management and response material are required, risk managers may seek to create an IMP as a supplement to the overall contingency planning document, forming the granular or tactical level requirements or responses that will direct crisis management activities, typically at the start of an event. The IMP should not be confused with the corporate- or program-level

contingency plans, as it is designed to assist with organizing immediate response protocols to practically support the often physical response to a crisis, rather than directly manage strategic-level or sustainable and complex response protocols. The IMP should provide outlines as to the nature of risks to place these into a context, and may have reduced or simplified components of the Business Continuity Management Plan as they relate specifically to the IMP. In essence, the goals of the IMP are to provide a series of succinct response sheets and questionnaires, enabling management to fall back on established protocols and procedures during the initial stages of a crisis event to allow them more time to focus on the unique requirements of a situation, rather than those that can be predicted ahead of an event. The contingency planning measure of the Business Continuity Management Plan is more of a corporate policy document, providing overarching rather than granular-level details. Contingency planning measures should be reviewed and appropriately modified throughout the life span of the activity, seeking to deter, detect, delay, and respond to the range of threats the company faces.