



# Intel Business Continuity Practices

As a global corporation with locations and suppliers all over the world, Intel requires every Intel organization to embed business continuity as a core business practice. By integrating business continuity as a core business practice in all decisions and programs, Intel is able to maintain and regularly test business continuity plans for all its sites, facilities and operations. In the event of a business disruption, our business continuity plans are designed to enable us to continue critical business functions (such as handling customer orders, overseeing production and deliveries, and managing the supply chain).

## Our business continuity plans include (but are not limited to):

- Relocating impacted businesses to designated recovery locations.
- Deploying redundant processing capacity at other locations.
- Developing procedures and systems designed to support recovery processes for critical business functions.
- Activating business continuity and technology teams tasked with managing the recovery process.
- Maintaining communications to ensure that Intel employees receive emergency notifications and instructions via a variety of sources, including in-building announcements, internal and external websites, and toll-free telephone numbers around the world.
- Testing our emergency and recovery procedures on a regular basis.
- Conducting annual assessments of each Intel organization's business continuity program.

## Intel business continuity principles

Five core business continuity tenets guide Intel's expectations for Intel organizations and our annual assessments of their success in meeting them.

1. **Management commitment.** We require clear ownership of the business continuity function the full of each group's general manager. This means maintaining the business continuity program as a core business practice, providing resources to support ongoing business

### Intel business continuity at a glance

- Business continuity is embedded and sustained as a core business practice.
- Crisis management and recovery plans are integral to doing business at Intel.
- Every Intel business group is required to have an active business continuity plan for their core business functions and processes.
- Business continuity plans are tested regularly as a continuous improvement process.
- Employees are trained on plan response.
- Regular assessments are required for response and recovery plans.
- New and emerging risks are integrated as part of sustaining program.

continuity strategy and activities, and management participation in business continuity activities, oversight and reviews.

2. **Risk and impact assessment.** We insist that every Intel organization document, review and update annually Risk and Impact Assessments for core business functions. This includes developing a Risk Mitigation Plan and having it ratified by the general manager and senior management.
3. **Prepared business continuity response.** We ensure that every business group has documented emergency response plans and business recovery plans, including response and recovery team structures and an activation process. New risks and impacts to the business must be integrated into each group's business continuity plans as they arise.
4. **Tested business continuity response.** We require business groups to execute drills to ensure the completeness of business continuity plans and to prepare the organization to perform effectively in a crisis. Groups must also perform annual self-assessments to identify and close gaps. Integrated drills with other Intel organizations are also frequently performed.
5. **Documented crisis response.** We have every Intel organization ensure it has a documented capability to manage a crisis, connect site recovery teams to the group-level crisis management team, and communicate appropriately with Intel Corporate Communications, suppliers and customers. We also a post-mortem process after all real events to identify gaps and document learnings.

## Business continuity is vital to our business

The nature of Intel's business has always dictated comprehensive emergency management practices and recovery plans. Since 9/11, Intel's Business Continuity (business continuity) Program Office has been directly sponsored at a corporate level by the executive office to ensure adequate senior management engagement and oversight. Intel's approach to business continuity is thorough and includes continuous support from the top down to ensure the highest level of preparedness possible. Business continuity planning is a consideration in every product's life cycle and everything we do — from factory design and manufacturing to operations and training.

## Intel's approach to business continuity

Intel's methodology focuses on impacts. We do not create business continuity plans specific to earthquakes, fires, computer viruses, tsunamis, power outages, manufacturing and supply line issues, or wars (though we have developed specific preparations for pandemics). Instead we focus on anticipating and mitigating the impact of any crisis, ensuring we can keep business going with no or minimum impact to our employees, customers, suppliers, and shareholders alike.

Our approach is to:

- Identify and validate key business functions and significant vulnerabilities
- Focus on business impact versus threat
- Build capability, resources and processes to respond to various business impacts effectively
- Focus on short- and long-term impacts
- Assess risks and initiate actions intended to minimize risks and their potential impact
- Proactively reassess new risks and potential impact
- Update plans and capabilities as warranted



## Ensuring “business as usual” in unusual times

To enable Intel to continue business operations in an environment of heightened threat, and quickly respond to emergencies and changing circumstances, we have:

- Created a Corporate Emergency Operations Center to coordinate multi-site emergency response.
- Established Site Emergency Operation Centers worldwide.
- Formed a Corporate business continuity organization to drive overall business continuity efforts and expectations.
- Integrated business continuity into the organization’s business practices and key business functions to enable timely recovery.

## We practice business continuity daily

Intel’s business continuity plans are ‘living’ documents. Each Intel organization is responsible for conducting quarterly drills to test their business continuity plans, identify gaps, and close them. Intel’s comprehensive annual environmental scans involve participation by executive staff including our chairman and CEO. This enables us to thoroughly review – and as appropriate – enhance our business continuity plans based on new business conditions, environmental changes, and emerging global threats. Intel’s business continuity plans are subject to audit and review by our Board of Directors.

We ensure business continuity excellence throughout Intel by:

- Making business continuity a fundamental business process and core discipline
- Including business continuity as an integral part of operations and our commitment to the Intel® Customer Excellence Program (CEP)
- Evaluating an Intel organization’s business continuity program as a key element in all Intel Quality Award (IQA) applications.

## Our record speaks for itself

Our record in dealing with crises in recent years attests to the effectiveness of this methodology. Among the threats we’ve faced over the last 10 years are:

- Sequel worm
- East Coast power failure
- Southeast Asian tsunami
- SARS
- Supplier fire
- War in Israel and Lebanon
- Typhoon Xangsane
- Hurricane Katrina

In each case, due to the response of our business continuity organization, none of our production lines had to be shut down, and there was nearly zero customer impact worldwide.

## Pandemic planning

After SARS, Intel began tracking the avian influenza for pandemic potential in 2004. The world is presently in phase 3 of a pandemic alert. This means a new influenza virus subtype is causing disease in humans, but is not yet spreading efficiently and sustainably among humans. Experts at the World Health Organization (WHO) and elsewhere believe that the world is now closer to another influenza pandemic than at any time since 1968, when the last of the previous century's three pandemics occurred. Currently the risk is low to Intel employees, but Intel believes a pandemic represents enough of a special threat that it mandates specific precautions and preparation.

Here are Intel's guiding principles in preparing for this threat.

- Continue to promote a healthy environment through good health practices.
- Minimize the spread of infection by partnering with local governments and public health organization, such as the World Health Organization (WHO) and Center for Disease Control (CDC).
- Implement a staggered deployment strategy based on risk and need at each location/geography.
- Maintain business continuity by developing the correct level of coordination and contingency planning.
- Treat people with dignity and respect through communication and transparency.

Intel's pandemic preparations include:

- Purchasing a generic Pandemic Preparedness Protocols published by International SOS (ISOS) Nov. 2005.
- Assembling a global multidisciplinary team to outline an implementation plan for response based on WHO Pandemic Phase and local risk.
- Developing pandemic response guidelines that include everything from hygiene procedures and personal protective equipment to covering everything from point-of-entry screening, communications and travel safety.
- Training each major business unit's business continuity manager on pandemics and Intel's response plans.
- Requiring all business units to complete drills based on a possible pandemic and use what's learned from these drills to improve our readiness, response and recovery capabilities.
- Setting up an employee 1-800 emergency line and emergency call center support that will activate to help employees and their families with medical information and other support.
- Determining minimum staffing levels and ensuring that individuals with key knowledge have backups.
- Having all groups assess their plans with the possibility of a closure of their workplace for from 10 days to 3 months.
- Ensuring critical staff has the ability to work effectively remotely.
- Planning for additional remote access capabilities and increased demand on telephone services.
- Developing an IT plan for identifying all critical work and giving employees who support this work priority access for working remotely.
- Notifying all critical suppliers of the possibility of a pandemic and making sure they have appropriate business continuity plans in place.
- Communicating with suppliers who have contingent workers on our sites to make sure they understand our site response and expectations.

- Identifying alternate locations for shipping in the event of a closure of a warehouse or facility.

## Employee personal preparedness

Intel's most valuable assets are its employees. That's why, in addition to training employees on an organizational level to handle crises, we also provide training and advice for dealing with them on a personal level.

An important thing to remember is that disasters strike quickly and without warning. They can force local evacuation or confine employees to their homes, offices, or somewhere else. What's more, no matter how well a community has planned its response to a disaster, a community's resources can quickly become overwhelmed in the event of a large-scale incident. For these reasons, a key component of Intel's Security & Safety Initiative (SSI) is to encourage employees and their families to prepare for emergencies through a Personal Readiness and Emergency Plan (PREP).

These plans are designed to help:

- Ensure the safety of employees' families
- Avoid interruption to work
- Help Intel continue meeting its obligations to customers, stockholders, and the rest of its employees

Each employee is asked to go through a four-step process for personal preparedness.

1. Assess - Discover local risks and potential consequences.
2. Prepare - Develop a Personal Readiness and Emergency Plan (PREP) that includes preparedness at work, home and car.
3. Practice - Practice and perfect the plan.
4. Respond - Implement the PREP in a time of emergency.

## Corporate communications for employees

When a disaster strikes, one of the most important things is establishing a communications channel for employees, their families, and the company as a whole. Employees onsite want to connect with families as quickly as possible. Employees at home or elsewhere will want to communicate with the company. Intel has a variety of emergency communications channels, including toll-free telephone numbers and the Internet.

In addition to the general communications channels listed above, Intel also has specific communications channels to work with those individuals and their families who are directly impacted. These channels include:

1. **Employee Assistance Program** - The program provides Intel employees and their dependents short-term professional counseling services at no cost. In an emergency, additional counseling resources are activated as needed.
2. **Intel Travel** - If an emergency occurs while employees are traveling for Intel, the travel office help reroute their travel and get them home.
3. **Relocation** - Intel's relocation services help employees who are temporarily relocated due to a crisis.



## **Working at home or away**

Many of Intel employees are issued laptops, cell phones or other personal computing and communications devices. These employees are instructed to carry these devices with them at all times so that they can be prepared and respond in an emergency. Having these devices with them ensures the ability to continue to work from off-site locations.

## **Intel business continuity in action**

Through Intel's rigorous business continuity (business continuity) planning, Intel strives to prevent injuries to employees, visitors and neighbors; protect Intel's assets from damage or loss; and minimize the effects of any incident so that they do not compromise our ability to achieve Intel's mission. The effectiveness of our business continuity program has been proven numerous times in real-life crises. How did we do? Here's a look at just three examples.

### **2006 Israel-Lebanon conflict**

When Hezbollah fired rockets and mortars at Israeli military positions and border villages on July 12, 2006, it was a big concern for the entire world and particularly for Intel. We have many employees in Israel as well as in Lebanon. In Israel, the expansion of our operations there — including the Israel Development Center (IDC) center located in Haifa in the North near the Lebanon border — make us one of the largest high-tech companies in the country.

The rocket attacks triggered Intel's Israeli site-wide Emergency Operations Center (EOC) and the EOC of our only impacted site, the Intel Israel Development Center. The site invoked their Alternative Workspace Plans and was able to accommodate alternative office spaces for many of the Haifa employees while approximately 1,200 worked from home. An emergency website and 1-800 hotline provided daily updates to employees. By spreading employees into various sites and homes, we were able to decrease risk. Many Intel families living beyond the hostilities offered to host northern employees. A summer camp was organized for kids. Intel's Israel operations stayed fully functional with minimum productivity impact—a good showing for Intel's business continuity program in Israel.

In Lebanon, we were able to manage key shipments and mitigate customer impact by invoking our business continuity plans, communicating with customers, and creating alternate means for delivery.

### **2005 Hurricane Katrina**

When natural disaster strikes, the scope of damage can be overwhelming – even if it doesn't affect your company directly. At Intel, managers quickly formed teams to organize the thousands of employees who called in to help and coordinated a wave of donations of equipment and skilled volunteers. The company provided organization and deployment of everything from money and skilled workers to an experimental wireless (WiMAX) network. Intel helped set up 150 relief sites with enterprise-class access points, coordinate the donation and deployment of 4,000 laptops, and

reconfigure desk-side phone equipment at Folsom to create a virtual call-center for collecting money during the "Shelter from the Storm" concert and fund-raiser. Intel and its employees also donated \$7 million dollars to the relief effort. Intel business continuity plans were at the core of executing these efforts, and the company profited from the real-life testing of these plans.

### **2005 subcontractor fire in Taiwan**

A fire in a subcontractor's facilities on May 1, 2005 threatened to create immediate supply issues for certain Intel Flash products and chipsets. At the time, this particular subcontractor accounted for 30% of the Flash factory assembly loadings and 30% of Intel's "Southbridge" chipset loadings. Executing a fast business continuity response, multiple groups from Intel's Technology Manufacturing Group were able to work together to radically decrease the impact of the fire from approximately 16 million Flash units to just 500,000 units. They also prevented a potential chipset gap of 5.4 million units. Overall, the team erased a potential \$1 billion impact to Intel on chipsets and helped the Flash Product Group meet a their second quarter Q2 revenue plan of record (POR) for 98 million units. The team's efforts included overcoming the challenge of replacing production of 31 sole-source line items.

### **Our business continuity efforts never stop**

As a global corporation, we take our commitment to our customers, shareholders, employees and suppliers very seriously. Consequently, in the belief there is much to learn from others, we regularly hold business continuity forums, inviting companies both within and outside our industry to share their approach and insights on business continuity. Attendance at these forums by our management and employees ensures a cross pollination on the best practices in business continuity between our industry and others, enabling us to better recognize and prepare for a wide variety of business disruption risks.

Although Intel has developed and deployed a comprehensive business continuity program, we cannot guarantee or provide any absolute form of assurance that our operations and systems will always be available or recoverable after a disaster or other major disruption to day-to-day business. No one really can. We do believe that the steps we have taken in our business continuity planning meet or exceed many of the best practices for business continuity in our industry and others, and will prepare us well for nearly any crisis we face.

## Frequently asked questions on Intel's business continuity program

In 2002, as part of our Security & Safety Initiative, Intel initiated a Corporate Business Continuity (business continuity) Office. Their mandate was to ensure business continuity became a core business practice at Intel. The overall goals of these efforts include making certain business operations continue during a wide range of threats and that the company can quickly adapt to changing circumstances and the potential requirements of emergency response. Here are our answers to questions we are frequently asked about our business continuity program.

### **Q1: What is Intel's Security & Safety Initiative (SSI)?**

**A1:** The Security & Safety Initiative (SSI) was chartered in 2001 by Intel Chairman Craig Barrett to oversee and coordinate security and safety for Intel's employees, as well as update Intel's Emergency Response Plans worldwide in light of the heightened threat environment. The goal was to expand emergency response plans and preparedness across all major business groups and critical functions. The Security & Safety Initiative ensures that business continuity (business continuity) is embedded in Intel's everyday way of doing business. SSI is driven by a virtual organization composed of senior management representatives focusing on Intel's commitment to business continuity, ensuring sufficient oversight, accountability and support for a solid business continuity program addressing new business challenges and changing environments.

According to Intel's philosophy, the success of its business continuity program depends heavily on the leadership and determination of senior management to be prepared for crises that could disrupt business. As leaders of the organization, the job of the senior management is to:

- Create the organization's business continuity strategies.
- Ensure the program is resourced from both a financial and a personnel perspective so that it can be successfully implemented and sustained.
- Demonstrate continuous commitment to business continuity.

### **Q2: How committed is senior management at Intel to business continuity?**

**A2:** Extremely committed. SSI is driven by a collection of senior managers representing all major Intel organizations. These senior managers are charged with keeping Intel's critical business running and recoverable by aligning the groups that drive security, safety and recoverability to provide direction and oversight of relevant corporate programs. These senior managers recognize that Intel identifies business continuity as a significant part of its corporate business principles and act accordingly.

### **Q3: What is business continuity?**

**A3:** Business continuity is an integral approach to doing business designed to ensure a company can keep its core business running during times of unexpected events or disasters. It includes:

- Laying the groundwork by defining the critical functions, intelligently assessing threats and their impact, mitigating the risks, and planning the best response for the business.
- Organizational communication and leadership during an event, as well as emergency response management to ensure staff functions effectively at all levels, and in all geographies.
- Speedy response to get back to normal operating conditions as soon as possible with minimal loss.

**Q4: How does business continuity differ from everyday problem management?**

**A4:** Business continuity differs from normal, everyday problem management in that the events and disasters are bigger; they often come with little warning; and, they often require resolution under intense scrutiny from both inside and outside the corporation. We may already be prepared for some localized events, but we need to ensure that we are equally prepared to address events and disasters that can ripple across multiple Intel sites or business groups and last for extended durations.

**Q5: What are the corporate expectations of Intel organizations in adopting business continuity practices?**

**A5:** Business continuity is a significant part of Intel's Corporate Responsibility (CR). The business continuity as a corporate mandate states that:

- Intel recognizes that a wide variety of disasters or failures can occur. However, through effective planning, you can reduce both the duration and severity of any such event. Intel strives to prevent injury to employees, guests, and neighbors; protect Intel assets from damage or loss; and minimize the effects of any incident, so that they do not compromise Intel's ability to achieve its mission.
- To accomplish the goals of preventing injury, protecting assets, and minimizing the impact of any incident, Intel operations incorporate business continuity as a core business practice.
- Business continuity is an integral approach to doing business, which ensures that you can respond to emergencies and keep the core business running during times of unexpected events or disasters.

**Q6: What business continuity expectations will there be on a regular basis?**

**A6:** Intel organizations will be expected to:

- As part of an existing planning cycle, regularly review, exercise and improve business continuity plans
- Undergo audits on a regular basis to ensure compliance
- Analyze new business functions/processes in terms of business continuity as they are being developed.
- Ensure appropriate risk reduction and business continuity plans are developed and implemented as each business function is being implemented, not after the fact.

**Q7: What are some of the key considerations an Intel organization is required to think through in developing a business continuity process?**

**A7:** The process of developing a robust business continuity process usually includes:

- Determining the top 3-5 business priorities. This is done at a staff-level and rippled throughout each Intel organization. An overriding consideration is that Intel's top priority is the security and safety of its people.
- Thinking about threats/risks broadly, then setting priorities and filling the biggest gaps first.
- Considering impacts in all areas needed to run the business — computer applications/data, physical site infrastructure, people impacts, customer impacts, supplier impacts, and intellectual property impacts.
- When mitigating risks and impact, making choices that are cost-effective and give consideration to risk vs. reward (i.e., some options may be too expensive given the return on investment that would be required).
- Knowing suppliers' plans (both internal and external suppliers/service providers).
- Setting customer expectations appropriately.

- Training staff and role modeling the behavior. Business continuity isn't a one-time effort, and it's more successful and easier when everyone knows what to do. Disasters shouldn't be the first test of a company's readiness/response capabilities.

**Q8: What has changed about emergency response thinking since 9/11?**

**A8:** Prior to 9/11, most of Intel's Emergency Response Plans favored single-site emergencies and/or short-term incidents. In today's threat environment, we obviously must be prepared for multi-site and longer-term outages, considering events that may last for months or even unknown durations.

**Q9: What is Intel doing to ensure it is prepared for a pandemic event?**

**A9:** Intel continuously monitors world events and issues to appropriately mitigate or deal with them. Since the SARS events in 2003, a pandemic event has been on our radar. A pandemic response, whether due to avian flu or another pathogen would use existing emergency response and recovery processes, as our capabilities are not restricted to particular events. In fact, the SARS event allowed us to refine the processes for a pandemic, and as a result, we have faster and more effective response capabilities across our organization.

Pandemics have also been one of the events which we have drilled. Pandemic planning is well understood with good alignment between various organizations and the Corporate business continuity Office.

Our response to a pandemic will be staged and vary based on the level of risk or response at a given time. If a pandemic reaches late Phase 5/Phase 6 (severity classifications from the World Health Organization), there will be lots of unknowns. We are consequently designing our response to be flexible so we can react quickly as the situation changes.

**Q10: What is Intel specifically concerned about and planning for in regards to a pandemic?**

**A10:** The potential impact of a pandemic includes:

- Reduction in staffing (30-50% for extended periods) for a variety of reasons, including sickness, death, child care, public health restrictions
- Employees or family members ill, employees afraid to come to work, quarantine of an employee's living area
- Closure of work places by public health officials
- Reduction in flights/air cargo capacity
- Travel restrictions
- Border closure
- Supply chain impacts

Our pandemic drills consider a variety of these impacts in multiple key sites. We have developed corporate level pandemic scenarios which have been used in drills across all major Intel organizations.