Avnet Business Continuity Program Overview

(Externally Releasable)

Contents

Introduction 2
Avnet – Who we are 2
Enterprise Risk Management 2
Enterprise Risk Council 2
Avnet's Business Continuity Program 3
Response Planning 3
Emergency Notification 3
Standards based approach 3
Response Organization Structure 4
Corporate level teams 5
Site or facility teams 5
Disaster Recovery (Information Technology systems or IT) 6
Conclusion 6

Introduction

We cannot assure that rapidly changing world events will not impact our business or yours. We can, however, assure you that Avnet has been and continues to be prepared to respond quickly to business interruptions or emergencies. Avnet will work with our valued suppliers and business partners to meet our customer needs while protecting our workforce and facilities.

The purpose of this Business Continuity Overview is to provide our customers and business partners with an understanding of Avnet's approach to Enterprise Risk Management and Business Continuity. Details of specific response plans are confidential due to the nature of our business and need for customer privacy. If additional details are required, contact our Business Continuity Program office for additional support (contact information at the end of this document).

Avnet – Who we are

Avnet, Inc. (AVT) is a Fortune 500 company who provides cost-effective services and solutions vital to a broad base of more than 100,000 customers and 800 suppliers. Avnet markets, distributes, and adds value to a wide variety of electronics components, enterprise computer products and embedded subsystems. Through our premier market position, Avnet brings a breadth and depth of capabilities that help its trading partners accelerate growth and realize cost efficiencies.

In addition to its core distribution services, Avnet markets, adds value and creates demand for the products of the world's leading electronic component suppliers, enterprise computing manufacturers and embedded subsystem providers. Avnet brings a breadth and depth of service capabilities, such as supply-chain and design-chain services, logistics solutions, product assembly, device programming, and computer system configuration and integration.

Avnet, with its innovative and entrepreneurial spirit, and its passion for customer service, assures customers and suppliers that they have chosen the right partner to accelerate their success.

Enterprise Risk Management

Avnet's Enterprise Risk Management (ERM) program regularly evaluates, prioritizes, and develops risk assessments and mitigation plans to address the various risks we may encounter as a global organization. This program ensures we provide the Avnet Board of Directors with the necessary information to fulfill its risk oversight role. Our Risk Management program is anchored by a cross-functional Risk Council composed of executives from every major business unit and is led by Joseph Burke, Vice President, Treasury and Enterprise Risk Management.

Enterprise Risk Council

The Risk Council is focused on identification and monitoring of current and emerging risks. The council's responsibilities are:

- To meet twice-yearly to address current and emerging risk factors
- Identifying and evaluation of enterprise risks of all types: financial, operations, physical and man-made
- Establish risk policies and ensuring they fall within Avnet's risk tolerances
- Evaluating and controlling risks to our global infrastructure, both physical and Information Technology support
- Ensuring proper reporting of risks to ensure compliance with policies and legal requirements

The ERM program office is responsible for monitoring progress on risk response plans and ongoing mitigation actions or remediations.

Avnet’s Business Continuity Program

Avnet has implemented a Business Continuity Management system for addressing potential risks to our business and minimizing recovery from business interruptions. The goal is to build resilience and effective management of recovery or continuity of business in the event of a disaster. The program is designed based upon our operational requirements and includes risk assessments, business impact analyses, recovery strategy development, detailed emergency response procedures, business restoration procedures and priorities, IT Disaster Recovery plans, and training validation exercises.

Response Planning

Business Continuity Plans have been developed to address the top ranked threats for each key location from all sources:

- Natural disasters (earthquakes, floods, fires, severe storms and hurricanes)
- Man-made disasters (power outages, hazardous material spills, geopolitical events)
- Systems, hardware, network, and software failures/outages

Avnet realizes that any loss of service to our customers could have substantial impact. Avnet mitigation and recovery plans are designed to recover from three levels of disruption along with corresponding escalation procedures to ensure adequate resources to recover with minimal disruption to business operations:

- Level 1 – Short-term 24-Hours or less (local resources)
- Level 2 - Medium (local and possibly regional resources)
- Level 3 – Long-term (full-company response)

Emergency Notification

In the event of any emergency situation or an event causing an outage of more than 24-hours (Level 2 - Medium) or Level 3 (Long-term) stage, Avnet’s Global Security Operations Center has the ability to use an Emergency Notification System (ENS) to send timely emergency communications to employees around the world. The GSOC watch-team has the ability to track message delivery and confirmation status in real-time to ensure critical personnel are notified of an emergency situation. This comprehensive emergency mass notification system will help keep all individuals informed before, during and after incidents in a timely and reliable manner.

Standards based approach to planning

Avnet’s Business Continuity Program is not currently certified to ISO 22301 standards; however we do follow many of the key tenets established by the ISO standard in the design and operation of our program. Clauses we utilize in our Business Continuity Planning:

- Clause 4: **Context of the organization**
  - Alignment of the Business Continuity Policy and Corporate policies to ensure synergy with Avnet’s Mission, Values, and Objectives
- Clause 5: **Leadership**
  - Continual communication with senior executives and board members on the status of our program and risk assessments based on current operations
  - Setting goals for achievement and ensuring we reach expected levels of performance
  - Setting standards and communicating changes for our global organization
- Clause 6: **Planning**
  - Establishing consistent polices, templates and vernacular for use in Crisis Management and Business Continuity activities
  - Monitoring progress to ensure compliance with agreed upon metrics
  - Integration of Crisis activities to ensure smooth transition to Business Restoration
- Clause 7: **Support**
  - Ensuring proper staffing, tools and training are available for our facilities across the globe

- Clause 8: **Operations**
  - Risk Assessments, Business Continuity strategy and procedure updates
  - Exercise and testing to ensure proper training and tools are in place
- Clause 9: **Performance evaluation**
  - Establishing metrics and internal evaluation with our Global Audit team to identify not only gaps, but best practices
- Clause 10: **Improvement**
  - Ensuring continual improvement, updates, and lessons learned from both real world and testing/exercises are incorporated and shared across all business units of Avnet.

Secure resilience management

Avnet utilizes a cloud-based secure application for hosting our Business Continuity plans. This application is customized to Avnet's needs and assist us in building, maintaining, and implementing a fully integrated crisis management and business continuity/disaster recovery program. These standardized plans cover essential facilities, regional, and corporate level response plans, response teams and resource requirements. Utilizing a central application provides global access and awareness of the necessary recovery actions needed for any key facility. This application provides a high level of standardization for our incident response procedures and establishes a common language across a truly global organization with locations in over 40 countries. These attributes promote quick response with minimal confusion to deal with often chaotic and potentially life threatening events.

The Business Continuity Plans (BCP's) are living documents that continue to be updated and adapt to changing business or environmental conditions. The BCP's contain information and procedures required to restore business operations in the event of an unanticipated interruption of normal operations or a serious business disruption (or the threat thereof) affecting the operation of our key functions. The BCP's articulate the action points where alternate business processes need to be deployed, the steps to deploy alternate business processes, resource requirements based on the level of threat/interruptions, and the methods for verifying the business has been properly restored. Business restoration and validation includes ensuring data integrity and associated activities for returning to "normal" business processing.

Essential elements of Avnet BCP's:

- Site specific Business Impact Analysis (BIA's)
- Risk assessment and threat profiles
- Notification, escalation, and declaration process
- Step-by-step Crisis Management and Incident Response and Recovery playbooks
- Essential vendor contact information
- Exercise and testing history
- Audit history for each plan

Each BCP Plan Owner, under the leadership of the Enterprise Risk Management PMO, maintains and reviews their BCP's at regular intervals to ensure its accuracy and effectiveness at restoring the business processes at the facilities. It is the responsibility of Avnet Executive Management, the ERM PMO, and the site BCP leads to ensure BCPs are kept up-to-date and team members are trained and are aware of their roles in an incident.

Response Teams

The BCP documents identify response and recovery teams, critical vendors, and outlines the different phases of recovery actions and detailed process playbooks. The following standardized roles and teams have been created as a guide (some regions may have different names, but the BCP will associate the local name with the standard teams for consistency):

Corporate level teams

Global Security Operation Center - Avnet's Global Security Department provides opensource intelligence updates, incident updates, and facilitation of crisis management calls and communications. These messages are pushed to email groups, phones or text messages by the 24/7 Global Security Operations Center watch team.

Corporate Crisis Management Team (CCMT) - This team is comprised of regional and corporate subject matter experts and provides strategic oversight and support to the Site Incident Management Teams. The CCMT reports up to Avnet Senior Executive Management and is charged with strategically assisting in maintaining operations and assets in the long-term and maintaining a corporate reputation and standing in the industry. Each person on the CCMT has a unique communication path within their respective chain of command.

Site or facility teams

Site Incident Management Team (SIMT) - This team is responsible for ensuring employee protective actions are being taken and has overall responsibility to manage crisis events at the site level, and to establish the recommended organization, actions, and procedures needed to:

- Recognize and respond to an incident
- Assess the situation quickly and effectively, determine if the BCP must be activated
- Notify the appropriate individuals and organizations about the incident
- Organize the company's response activities, including activating a command center
- Escalate the company's response efforts based on the severity of the incident
- Protect employees
- Communicate conditions, necessary details, and next steps to the Corporate Crisis Management Team. SIMT will inform employees, critical stakeholders, suppliers and customers
- Minimize the total disaster financial loss to Avnet and/or customers

Crisis Management Team (CMT): (Many sites use a CMT in lieu of a SIMT)

- Team acts as the site incident oversight of response and recovery activities
- Coordinate communications both internally and externally
- Coordinate requests and logistics for response resources

Emergency Response Team (ERT)

- First on-scene to assess the damage caused by the disaster
- Ensure precautionary measures are taken in advance of any impending disaster
- If an evacuation is REQUIRED the ERT will assist in the evacuation of the facility and work with responding teams to mitigate the effects

Business Recovery Team (BRT)

- Lead the recovery and stand-up of the business operations in the original or alternate site
- Focus of the BRT is to get operations up and running within the RTO, identifying any shortfalls or complications/resource requests to the SIMT
- Team Leaders of the BRT will get updated status from the ERT and the RST to ensure prompt recovery of each department

Recovery Site Team (RST) (If required)

- Primary responsibility is to ensure that the **alternate site** is ready, and adequate for arriving recovery team/s and personnel
- The RST will be the first at a meeting point or alternate site, responsible for set up and direction to follow-on personnel and/or employees
- Provides support for both the physical site and technology issues regarding alternate site set-up and operations

Disaster Recovery (Information Technology systems or IT)

GLOBAL INFORMATION SYSTEMS (GIS) - Failure of any of Avnet's Information Systems could have an adverse material effect on our operations. A detailed GIS Data Center Disaster Recovery Plan is in place. Risk response plans have been developed establishing fully executable plans and mitigating actions in the following identified risk areas:

- Data Protection
- Steady State Protection
- Business Continuity Protection
- Site Environmental Protection
- Data Center Recovery Planning

CYBERSECURITY - Cybersecurity involves protecting Avnet's information and systems from cyber breaches, threats or attacks. The Avnet team maintains visibility to suspicious actions against our data, network, and systems and initiates actions to protect these assets and our brand. This includes a cybersecurity incident response plan. Avnet's security framework in support of this model focuses on the following:

- Security Intelligence
- Data Security
- Enterprise Identity Management
- Audit & Compliance
- Infrastructure Security
- Development Security
- Security Awareness Program
- Security Operations

Conclusion

Under the guidance of Avnet's Enterprise Risk Management Program Office, Business Continuity Plans have been developed with the goal of ensuring the continuity of our operations and minimizing the impact to all of Avnet's stakeholders should an emergency or significant business interruption occur. Disasters and significant business disruptions are inherently unpredictable, and we recognize the need to develop current comprehensive business continuity strategies to enable us to meet our obligations to our customers while first and foremost protecting the health and safety of all personnel.

Business Continuity and Enterprise Risk Project Management Program Contact

We trust you will find this document helpful in understanding Avnet's Business Continuity and Data Center Recovery Planning process. If you have additional questions contact the Avnet Business Continuity Manager and Enterprise Risk Management PMO:

Kelly Hughes, Senior Manager

- Kelly.hughes@anvet.com

Organizational Mailbox

- enterpriseriskmangement@avnet.com