Business Continuity Management (BCM) Customer Overview

Contents

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 and emergencies. Avnet will collaborate with our valued suppliers and business partners to meet our customer needs while protecting our workforce and facilities.

The purpose of this Business Continuity Management overview is to provide our customers and business partners with an understanding of Avnet's approach to Enterprise Risk Management and Resiliency.

Avnet – Who We Are

Avnet, Inc. (AVT) is a $26.5 billion (FY23) Fortune 500 company with 15,800 employees across the globe who provide cost-effective services and solutions vital to more than 1M+ customers. With over 247B+ units shipped annually, Avnet markets, distributes, and adds value to a wide variety of electronics components, enterprise computer products, and embedded subsystems.

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. The program ensures we provide the Avnet Leadership Team and Board of Directors with the necessary information to fulfill their risk oversight role. The program manages our risk exposure through a Risk Council that is composed of leaders from major business units across Avnet and is sponsored by the Avnet General Counsel and Chief Legal Officer.

Risk Council

The Risk Council's responsibilities are:

- Meet twice-yearly (September and March) to address current and emerging enterprise risk factors
- Identify and evaluate enterprise risks of all types: financial, operations, physical, and man-made
- Recommend risk policy adjustments or controls to ensure identified risks fall within Avnet's risk tolerances
- Evaluate risks to our global infrastructure
- Ensure proper reporting of risks to confirm compliance with policies and legal requirements
- Identify ongoing risk controls or mitigation plans for each of the identified enterprise risks

Avnet's Business Continuity Management

Avnet has implemented a Business Continuity Management (BCM) for addressing potential risks to our business and minimizing the time to recover from business interruptions. This system builds resilience and effective management for crisis response and business recovery in the event of a disaster.

Avnet approaches business continuity based upon our operational requirements and includes risk assessments, business impact analyses, recovery strategy development, emergency response procedures, business recovery procedures and prioritization, testing, and training.

Avnet's ERM&R director works in close coordination with our Global Information Solutions team, who deliver innovative technology solutions, cost effective operational resilience, and robust security and controls.

Response Planning

Business Continuity Plans (BCPs) address the top ranked threats for each key location from all sources:

- Natural disasters (earthquakes, floods, fires, severe storms)
- 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 a substantial impact. Avnet mitigation and recovery plans categorize disruptions into three classifications:

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

Emergency Notification

In the event of an emergency situation or an event causing a Level 2 or Level 3 outage, the Avnet Global Security Operations Center (GSOC) has the ability to send timely mass communications to all employees impacted by a disaster or incident. This mass notification system will keep employees and leaders informed during and after incidents in a timely and reliable manner.

Standards Based Approach to Planning

Avnet's business continuity 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. Following are key elements we include in our plan development:

- Clause 4: **Context of the Organization**
  - Alignment of Business Continuity Management and corporate policies ensure synchronization with Avnet's Mission, Values, and Objectives.
- Clause 5: **Leadership**
  - Communication with senior executives 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 common to crisis management and business continuity planning and response teams.
  - Monitoring progress to ensure compliance with agreed upon metrics.
  - Integration of crisis activities to ensure smooth transition to business recovery.
- 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 training and tools are in place and meet the needs of the business.
- Clause 9: **Performance Evaluation**
  - Establishing metrics and internal evaluation reviews with our Global Audit team to independently verify compliance with policies, identify gaps, and share best practices across the organization.
- Clause 10: **Improvement**
  - Ensuring continual improvement, updates, and sharing lessons learned from exercises, tests, and real world incidents.

Avnet Business Continuity Plans

Avnet utilizes a cloud-based secure application for hosting our BCPs. This platform aids Avnet in the development, storage, and access to our crisis response and business continuity plans. Utilizing a cloud platform provides global access for the plans at the time of an incident, ensuring a timely and coordinated response to restore operations as soon as possible.

The BCPs are living documents and will continue to evolve and adapt to changing business or environmental conditions. The plans 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. These plans cover facilities, response teams, testing, exercise documentation, and playbooks for crisis management and business recovery activities.

Essential elements of Avnet BCPs:

- BCP owners and business leaders for the facility
- Site specific Business Impact Analysis (BIAs)
- Risk assessment and threat profiles that take into account local threats/risks
- Notification, escalation, and declaration process
- Crisis Management and Incident Response playbooks
- Business Recovery Procedures (in the BCP or other systems used by our distribution centers)
  - Establish the Return to Operations (RTO) for critical business operations, the maximum recovery time allowable before a disruption causes unacceptable damage to business
- Essential vendor contact information
- Exercise and testing history
- Audit history for each plan

Each BCP owner is responsible for maintaining and reviewing their assigned BCPs at regular intervals to ensure accuracy and effectiveness. BCP owners also work with facility leaders to keep team members trained and aware of their roles during an incident.

It is the responsibility of the ERM&R department to monitor and assist the annual review process, testing, exercises, and activations in addition to providing feedback to the Avnet internal Global Audit team. The Avnet Director of Enterprise Risk Management & Resiliency's contact information is at the end of this document.

Response Teams

The BCP documents identify response and recovery teams which are essential to crisis response and business recovery. The following is a list of standardized teams most commonly used across Avnet. Some facilities may have different names unique to their locations and those will be noted in each individual BCP.

Global Security Operation Center (GSOC)

The Global Security Operation Center (GSOC) integrates open-source intelligence and analytics with technology to monitor risks, improve incident response, and maintain compliance. They are the core component to mitigate external risks, protect corporate assets, maintain situational awareness, and safeguard personnel. The GSOC is the facilitator for our mass communications capability using the Crisis24 Risk Management Platform.

Corporate Crisis Management Team (CCMT)

This team is comprised of corporate subject matter experts and provides strategic oversight and support to the Site Incident Management Teams/Crisis Management Teams. The CCMT reports to Avnet Leadership Team (ALT) and is charged with strategically assisting to maintain operations and assets in the long-term and maintaining the corporate reputation and standing in the industry. Each person on the CCMT has a unique communication path within their respective reporting structures and/or business units.

Site Incident Management Team (SIMT)

This team is responsible for ensuring employee protective actions are 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 to determine if BCP activation is needed
- 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 CCMT
- Minimize the total disaster economic loss to Avnet and stakeholders

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

- Team oversees the 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
- Ensures precautionary measures are taken in advance of any impending disaster
- If an evacuation is ordered, the ERT will assist in the evacuation of the facility and work with responding teams to mitigate impact

Business Recovery Team (BRT)

- Lead the recovery and stand-up of the business operations in the original or alternate site
- Primary responsibility is to restore operations within the return to operations (RTO) timelines, identifying any shortfalls, complications, restoration time estimates, and resource requests to the SIMT/CMT

Recovery Site Team (RST) (If required)

- Stands up an alternate worksite and ensures it is ready for arriving recovery team/s and personnel
- Responsible for the direction of employees assigned to the alternate work site
- Supports the physical site activation and technology requirements for the alternate site

Disaster Recovery (Information Technology)

Global Information Solutions (GIS)

Failure of any of Avnet's information systems could have an adverse effect on our operations. A detailed GIS Data Center Disaster Recovery (DR) Plan is in place at Avnet.

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 an Avnet cybersecurity incident response plan. Avnet's cybersecurity framework 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 the Avnet Business Continuity Manager, BCPs have been developed with the goal of ensuring the continuity of our operations and minimizing the impact to all of Avnet's stakeholders. Disasters and significant business disruptions are inherently unpredictable, and we recognize the value of proper planning and business continuity strategies that enable us to meet our obligations to customers and protect the health and safety of all personnel.

Director, Enterprise Risk Management & Resiliency

We trust you will find this document helpful in understanding Avnet's Business Continuity Management. If you have additional questions please contact me.

Jeanine Buccola, Director ERM & Resiliency
ISO 22301 BCM Lead Implementor and Lead Auditor; DRI Certified Business Continuity Professional (CBCP)

jeanine.buccola@avnet.com