White Paper

Business Continuity Management

"SAS' Business Continuity Management initiative reflects our commitment to our employees, to our customers, and to all of the stakeholders in our global business community to be a responsible and reliable business partner."

The version of this paper is February 2020.

For more information about SAS' Business Continuity Management (BCM) initiative, send e-mail to bcmprogramoffice@sas.com

Table of Contents

Business Continuity Management

> "At SAS we develop enterprise-class analytics software that guides our customers' decisions about their business operations, their products and their customers. We also make an extraordinary investment in our employees, making us one of the top-ranked workplaces around the world. We extend this same vision and planning to manage risk in an increasingly interconnected and dynamic business environment. SAS' Business Continuity Management initiative reflects our commitment to our employees, to our customers, and to all of the stakeholders in our global business community to be a responsible and reliable business partner."
> Jim Goodnight, CEO of SAS

Business Continuity Management (BCM) refers to an organization's plans and procedures aimed at protecting its key assets and continuing its critical business functions in the event of anticipated and unanticipated threats. BCM takes into consideration corporate governance, information security, and corporate social responsibility, the primary factors that customers consider when selecting the strategic vendors to which they entrust their business.

SAS' global BCM program evolved from its longtime disaster recovery and crisis management procedures. Applying an all-hazards planning approach, SAS' incident preparedness and response is focused on protecting and recovering core business operations from threat impacts. Security, Facilities, IT, Communications, HR, Legal and the business units work together proactively to develop resilience and mitigation strategies. In a disruptive incident, they coordinate to execute response, recovery and business resumption plans. Under SAS' communicable disease plan, additional subject matter experts are engaged with the areas named above to coordinate proactive response activities in accordance with applicable government guidance.

The global BCM Policy provides a layer of program governance, formalizing roles and responsibilities and standardizing specific activities that include annual plan maintenance and testing, staff training, and management program review.

The main focal points for SAS' BCM program are:

- Protecting employees (life safety)
- Providing customer support
- Restoring the services upon which critical business functions depend.

Core program components

SAS' BCM program continues to develop in alignment with industry best practices and standards for business continuity. Key components of the program include:

- Executive oversight in risk management and program development
- Risk assessment and Business Impact Analysis (BIA)
- Impact mitigation and business resumption strategy development
- Business resumption plans to support recovery of critical business functions

- Emergency Operations Command (EOC) for disruptive incident management
- Annual plan maintenance, exercise, and staff training.

Plan contents

Typical BCM plans at SAS include:

- Incident notification/escalation process
- Roles and responsibilities of response, recovery, and business resumption staff
- Internal and external call lists
- Alternative site information
- Application and system dependencies
- Critical third-party supplier requirements and contacts
- Business resumption strategies (for example, where appropriate, critical functions will use manual workarounds, staff can work from alternate locations, critical function services can be provided from staff in other geographic locations).

A global approach to planning

SAS' BCM initiative extends to SAS' global offices. Its BCM methodology is applied corporate-wide, using standardized templates and processes for response, recovery, and business resumption planning, and using knowledge and resources at the local, regional, and headquarter-office levels. SAS office is responsible for developing and implementing plans in accordance with corporate standards to ensure an appropriate level of planning to meet business drivers while mitigating risks. A global collaborative approach to planning also supports the identification, development, and implementation of backup strategies for critical business processes and IT dependencies. This approach ensures a sustained minimum level of care for local and global customers so that if required, support may be provided from another office or from SAS Headquarters. Global communication protocols are in place to support impact assessment and activation of local incident management teams and SAS' corporate Emergency Operations Command.

Enhanced company resilience

In addition to supporting incident preparedness, the BCM program is also a catalyst for the ongoing improvement and increased resilience of SAS' operations. In the short term, key business processes are documented, internal and external dependencies are assessed, and, where appropriate, employees are cross trained for key roles within the organization.

However, a long-term result of SAS' BCM program is the improvement of business processes and enhanced company resilience because the ability to quickly recover from unforeseen incidents is closely tied to more efficient and effective day-to-day operations.

Customer support

SAS wants its customers to have the support they need to continue using SAS software on an ongoing basis. As such, SAS' Business Continuity Management planning is focused on services that must continue after a disruptive incident occurs. SAS' global recovery strategies for several key customer-facing functions are summarized below:

- **Communications** - During an incident, SAS may communicate with customers through multiple channels including: company phone messaging, the corporate website, social media, email, instant messaging, video conferencing, personal contact with account managers and other staff, and through business partners and the media.
- **Source code** - Copies of the SAS source code for all production products are kept on-site and off-site to expedite recovery. On-site copies are stored in a below-ground, fire-resistant vault. Source code and distributed media for major SAS software releases are archived.
- **Global hosting** - SAS provides SAS Cloud Analytics, delivered as software-as-a-service (SaaS), and enterprise hosting for customers worldwide who want to deploy SAS solutions rapidly. These solutions reside in secure data centers and are resilient to many types of potential incidents. As appropriate, regular off-site rotation of data backups or data replication is completed to allow for data restoration.

  For customers with more specific requirements, additional options such as off-site recovery offerings and recovery time guarantees are available. A Disaster Recovery Requirements Planning process is designed to help customers arrive at a solution that is cost-effective for their needs.
- **Licensing Operations** - SAS has designed and implemented measures to ensure that customer and software license key support will continue. This support can be provided through alternate methods and multiple channels that include recovery staff equipped to work from alternate locations.
- **Technical support** - In daily operations, SAS Technical Support provides 24x7 support for critical problems by routing the issues to Technical Support staff around the world during their normal business hours. This "follow-the-sun" support model provides a baseline strategy for global support during an incident. In addition, if SAS headquarters becomes inoperable, business resumption strategies include local staff working remotely and the transfer of responsibility to regional and global technical support staff.

IT recovery

SAS uses robust IT infrastructure housed in hardened, secure enterprise data centers. When an unforeseen incident occurs, there are plans in place to assess, restore, and resume normal operations for affected IT services.

Recovery procedures include restoring facilities (for example, buildings and electricity) and support services (for example, telephone service and computer infrastructure) to facilitate the recovery of critical business functions. Critical services are supported in multiple data centers, providing redundancy. The data centers are equipped with uninterruptible power supplies (UPS), diesel generators, multiple power feeds, and redundant switch gear for maximum reliability. All critical IT services are monitored and alerted automatically. SAS uses multiple internet service providers to provide Wide Area Network (WAN) network redundancy.

Many components of the IT recovery plan are exercised regularly, as they are the same procedures used in maintaining a complex infrastructure for daily operations. Recovering from system failures and restoring data subsystems are handled by on-call staff.

SAS Institute Inc. World Headquarters +1 919 677 8000 To contact your local SAS office, please visit: **www.sas.com/offices**