Global Business Resiliency (GBR) Program Policy

Table of Contents

1. Purpose

Cisco's Global Business Resiliency (GBR) policy ensures corporate focus on resumption of Cisco's business in the event of a business interruption.

2. Scope

This policy applies to all aspects of Cisco's business, all employees, all functions, including support functions and diversified business units, all locations, all subsidiaries and all acquisitions.

Cisco IT has resiliency capabilities in place and relies on information from the GBR program to ensure services adopt the appropriate capabilities. Through this alignment, Cisco IT will continue to ensure resiliency service level agreements are met in the event of a disruption that could impact the IT services supporting the organization, our customers and our partners.

And/or this policy includes the evaluation and consideration of external partners, vendors, and suppliers is within the scope of this policy; which will be based on the criticality of their support, products and/or services.

3. Policy Statement(s)

This policy must to ensure Cisco's ability to recover from business interruptions and to resume operations, ensure employee safety, and provide continued support for Cisco customers and partners

3.1 Cisco GBR Program Management

4.1.1 All Cisco function senior management must adopt the GBR program and framework and ensure all entities within the function comply with the GBR policy.

4.1.2. Senior management sign-off is required for all final BIA's, response plans, testing and remediation plans

3.2 GBR Business Impact Analysis

4.2.1 Each function must perform a risk threat assessment and business impact analysis to identify significant risks/threats and prioritize critical functions based on financial and non-financial impact to the organization.

4.2.2. All functions must identify critical process dependencies which include systems, applications, people, facility, vendor/supplier, and any other necessary resources to recover the critical function.

3.3 GBR Strategy and Plan Development

4.3.1 All critical functions, levels C1-C3, within Cisco must develop appropriate and actionable contingency plans that will enable management to focus on resuming Cisco's most critical functions, in the event of a business disruption. The plan shall have documented recovery strategies that include workarounds for processes in which dependencies are unavailable to resume servicing the customer.

4.3.2. All critical functions, levels C1-C3, must ensure key suppliers and partners supporting critical functions have effective contingency arrangements in place.

3.4 GBR Testing and Maintenance

4.4.1 Business Resiliency testing for all critical functions, levels C1-C3, must take place annually for all critical processes.

4.4.2. All Cisco Functions must review their BIA and BCP plans annually and when there has been a significant change in the business or infrastructure.

3.5 Monitoring and reporting of the GBR program to management Title

4.5.1 GBR program status reporting will be presented to Executive Management periodically and as needed.

4.5.2. Significant gaps/deficiencies in the program will be escalated to Executive Management representing the Senior Leadership team for remediation if unresolved and poses a threat to the organization's ability to adequately recover.

3.6 Training and Awareness

4.6.1 Business resiliency training applies to all Cisco employees, management and process owners involved in the execution of business continuity plans.

4. Policy Compliance

Policy compliance requirements are as follows:

4.1 Compliance Effective Date

This policy is effective June 2009 after final approval by the Executive Management.

4.2 Compliance Measurement

Compliance with Cisco's policies is required. Compliance to this policy is verified through various methods, including but not limited to, reports from available business tools, internal and external audits, self-assessments, and/or feedback to the policy owner.

4.3 Compliance Exceptions

There are no exceptions to this policy. No supplementary policy may supersede or negate any or all parts of Cisco's corporate GBR policy.

4.4 Non-Compliance

Deviations or non-compliance with this policy may result in disciplinary actions, up to and including termination, as allowed by local laws.

Compliance with Cisco policies is required. Deviations or non-compliance with this policy, including attempts to circumvent the stated policy/process by bypassing or knowingly manipulating the process, system, or data may result in disciplinary actions, up to and including termination, as allowed by local laws.

5. Definitions

The following terms and definitions are used in this document:

BCM	Business Continuity Management
GBR	Global Business Resiliency (Function within Cisco Treasury)
Diversified Business Unit	Various business models are used within Cisco, to include some business units that are not fully integrated across the functional organizations. These diversified business units are often recently acquired companies that, while a part of Cisco, are not integrated into the functional organizational model, and therefore not integrated into the functional contingency plans.
Functions	All Cisco business units
Program Documents	Guidelines, Framework, planning templates such as the BIA, Recovery Strategy, Recovery Plan, etc. and other necessary tools used for GBR