



Business Continuity Management & Disaster Recovery

Have You Conducted a Business Impact Analysis (BIA) Recently?

Contingency planning, also referred to as Business Continuity Planning (BCP), is about a coordinated strategy that involves plans, procedures and technical measures to enable the recovery of systems, operations, and data after a disruption. A Business Impact Analysis (BIA) is the foundation for building Contingency Plans.

Once the BIA is completed, Contingency Plans can be developed using the information identified in the BIA. For MIHS, two types of Contingency Plans will need to be developed. Emergency Mode Plans for business unit recovery and Disaster Recovery Plans (DRP) for Information Technology (IT) systems and infrastructures.

A BIA is a critical step in contingency planning. The critical steps for a BIA include the need to:

1. Identify business disruption events and measure probabilities
2. Identify critical business functions
3. Identify critical computer resources that support key business functions
4. Identify disruption impacts and allowable outage times
5. Develop recovery priorities

HIPAA REQUIREMENT

Contingency plan is a HIPAA Security standard. The objective of the contingency plan standard is to establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain EPHI. As shown in bold in Figure 1, the Contingency Plan standard is defined within the Administrative Safeguards section of the HIPAA Security Rule.

Standards	Implementation Specifications	R = Required A = Addressable
Contingency Plan	Data Backup Plan Disaster Recovery Plan	R R

	Emergency Mode Operation Plan Testing and Revision Procedure Applications and Data Criticality Analysis	R
		A
		A

Contingency plan related requirements are also identified as implementation specifications in the Physical Safeguards section of the HIPAA Rule as well as the Technical Safeguards section.

OUR BIZSHIELD™ METHODOLOGY

The Seven Steps to Enterprise Security is a methodology that describes a road-map to safeguard sensitive business information and enterprise vital assets. This methodology is also referred to as BizShield™. BizShield™ has also been influenced by the domains defined in the ISO 17799:2005 security standards as well as the CobIT and NIST security frameworks.

The BizShield™ methodology delivers *confidentiality, integrity and availability* (CIA) of your vital information and business assets. This methodology provides the blueprint for defending today's enterprise. The Seven Steps methodology provides the framework for addressing contingency requirements.

The BizShield™ security methodology identifies seven critical steps for an organization to follow as a twelve-month framework for organizing and prioritizing enterprise security initiatives.

OUR PROFESSIONAL TEAM

ecfirst only engages credentialed professionals for its BIA engagements. Credentials such as CISSP, CSCS and CBCP are typical of ecfirst Teams assigned to client engagements.

YOUR COMMITMENT TO US

- 1) Interviews with key members of IT staff, key individuals in departments and management.
- 2) Copies of IT system and network documentation including policies and procedures and inventory of vital assets such as servers and applications.

OUR DELIVERABLE TO YOU

A BizShield™ Business Impact Analysis (BIA) document will be created based on our review and analysis of information collected from your organization.

This BizShield™ Business Impact Analysis (BIA) Report will include information in the following areas:

- Business Risk Assessment
 - Key business processes identification
 - Time-bands for business service interruption management
 - Financial and operational impact
- Key Sensitive Systems and Applications Summary
- Emergency Incident Assessment
 - BIA process control summary for emergency incident assessment
 - Serious information security incidents
 - Environmental disasters
 - Organized and/or deliberate disruption
 - Loss of utilities and services
 - Equipment or system failure
 - Other emergency situations

Fixed Fee with No Expenses: Call for details and a customized proposal exclusively for your organization.

COMPLIANCE PORTAL SITE LAUNCHED

You are only 1-click away from major information security and business continuity related standards and key references at www.ecfirst.com/complianceportal/. Visit today.

COMPLIMENTARY EXEC BRIEF PDF ON CONTINGENCY PLANNING & BIA

For a complimentary executive brief PDF on Contingency Planning & BIA, please contact Nazeela Shokrai at Nazeela.Shokrai@ecfirst.com.

TESTIMONIALS

"The HIPAA Academy developed a comprehensive Business Impact Analysis (BIA) and Contingency Plan documents that met HIPAA Security Rule specifications and exceeded our stringent requirements. The work was executed professionally and their templates were detailed to capture small, yet critical information to establish recovery priorities."

David P. Walsh
HCF Management, Inc.

"Very informative and accurate."

Laura Bagus
Edward Hospital

About ecfirst

ecfirst delivers world-class information security, regulatory compliance solutions and its professional services team enables businesses address IT staffing challenges every day. With over 900+ clients, ecfirst was recognized as an Inc. 500 business – America's Top 500 Fastest Growing Privately Held Business in 2004 – our first year of eligibility. ecfirst assists organizations with their compliance initiatives for a secure information infrastructure that is compliant with regulations such as PCI DSS, HIPAA, Sarbanes-Oxley, ISO 27002, or federal and state legislations. ecfirst serves a Who's Who client list that includes technology firms, numerous hospitals, state and county governments, and hundreds of businesses across the United States and abroad. A partial list of clients includes EMC, IBM, Principal Financial, U.S. Army, U.S. Dept. of Homeland Security, U.S. Dept. of Veterans Affairs and many others.

Information Security & Compliance

ecfirst delivers deep expertise with its full suite of services that include Single Sign-On (SSO), context management, contingency planning/Business Impact Analysis (BIA), vulnerability assessment, as well as managed compliance, security and IT infrastructure solutions. ecfirst has successfully executed fixed price, fixed deliverable, turnkey projects across the United States.

World-class IT Professional Services

The ecfirst Professional Staffing Practice excels in meeting your short and long term requirements for contract professionals in the areas of Web development, system, database and network administration, application development, system architecture, and project management. This practice is distinguished with credentialed staff (PMP, CBCP, CISSP, CSCS, CHSS or others that may be required) that includes deep industry knowledge in the healthcare, financial, technology and government markets.

Compliance and Training Certification

The ecfirst compliance training program is exclusively endorsed by the American Hospital Association (AHA). The Certified HIPAA Administrator (CHA™), Certified HIPAA Professional (CHP) and the Certified HIPAA Security Specialist (CHSS™) certifications are the gold standards in the Industry. The ecfirst Certified Security Compliance Specialist (CSCS) Program is the first and only information security program that addresses all major compliance regulations from a security perspective.

Talk to [ecfirst.com](http://www.ecfirst.com) and you will find an organization that is passionate about the services we deliver and exceptionally devoted to its clients. For more information, please visit <http://www.ecfirst.com/>.