Contingency planning, also referred to as Business Continuity Planning (BCP), is 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. Typically, 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.

Compliance Mandate

Contingency Plan is a HIPAA Security Standard. It is also a Clause in the ISO 27000 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 the table below, 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	R
	Disaster Recovery Plan	R
	Emergency Mode Operation Plan	R
	Testing and Revision Procedure	A
	Applications and Data Criticality Analysis	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.

It Starts with a BIA

A BIA is a critical step in contingency planning. In a BIA we:

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.

Our *biz*SHIELD^{tm} Methodology

The Seven Steps to Enterprise Security is a methodology that describes a roadmap to safeguard sensitive business information and enterprise vital assets. This methodology is also referred to as *biz*SHIELD^{tm}. *biz*SHIELD^{tm} has also been influenced by the clauses (domains) defined in the ISO 27002 security standards as well as the CobIT and NIST security frameworks.

The *biz*SHIELD^{tm} 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 *biz*SHIELD^{tm} 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^{TM} 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 downtime procedures and inventory of vital assets such as servers and applications.

Our Deliverables to You

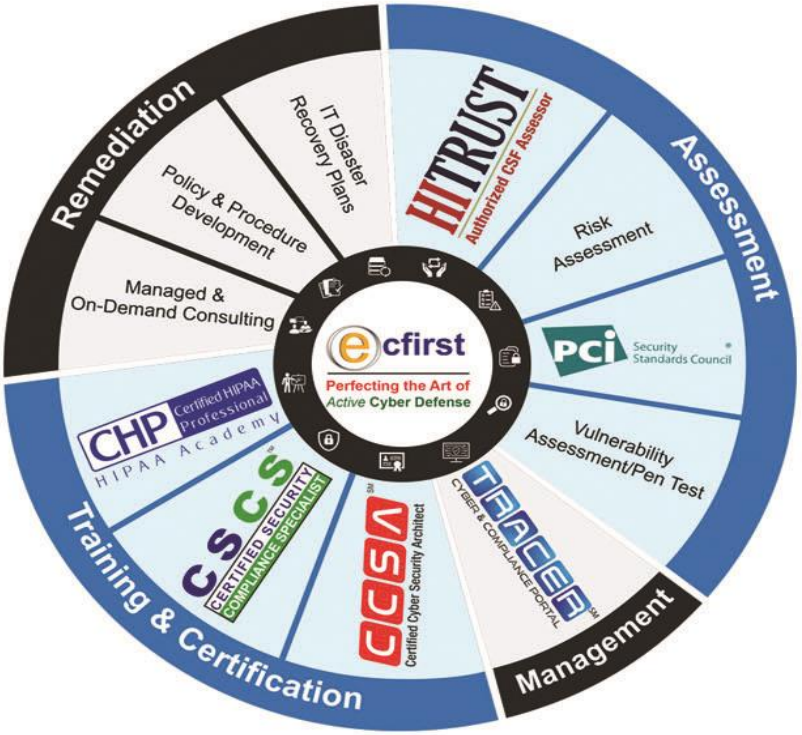
A *biz*SHIELD[tm] Business Impact Analysis (BIA) document will be created based on our review and analysis of information collected from your organization. This *biz*SHIELD[tm] Business Impact Analysis (BIA) Report will include information in the following areas:

- **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 a Monthly Payment Schedule: Call for details and a customized proposal exclusively for your organization. *On-Demand Compliance Solutions from ecfirst provides your organization with access to specialized compliance and security skills with no short term or long term commitments. Get Started Today!*

ecfirst

Perfecting the Art of *Active* Cyber Defense



Client Reference

"BrightOutcome is focused in improving patient health outcomes across the continuum of care. BrightOutcome is deeply committed to securing patient information across our systems and Web-based applications. We have been working with Ali Pabrai and his wonderful team at ecfirst since 2012."

"The ecfirst team literally helped us build our HIPAA practices from ground up, allowing us to offer secure HIPAA-compliant eHealth and health IT solutions to our customers across the U.S. We are actively taking the logical next step in working with ecfirst to pursue the HITRUST certification in order to further expand our market. We see the partnership with ecfirst as an ***integral part*** of our business strategy and have been ***extremely satisfied*** with the ***quality and value*** of the services that ecfirst has rendered."

BrightOutcome
COLLABORATIVE SYMPTOM MANAGEMENT

DerShung Yang | Founder & President

"I just wanted to take a moment and say thank you. Thank you and the ***excellent team*** at ecfirst for ***hard work***, late hours and ***diligence*** during the first round of our HITRUST certification, and now working on our annual risk management and HIPAA compliance assessment."

"We at BRG are always looking to improve and enhance our compliance and cybersecurity posture. This is an area of executive and strategic priority for our organization to secure confidential client information. From HIPAA compliance, cybersecurity pen tests, to the HITRUST certification engagement, we have found ecfirst to be an ***exceptional partner*** that labored incredibly hard for us, with us. The ecfirst insight and diligence to ensuring HITRUST certification mandates are met led to us completing our engagement on budget and time."

BRG
Berkeley Research Group

Chip Goodman | Vice President of Information Technology

John Schelewitz | John.Schelewitz@ecfirst.com | +1.480.663.3225

Delivering Everything Compliance. Everything Security.

1000s of Clients | Clients in all 50 States | Clients on 5 Continents

HITRUST Authorized CSF Assessor | PCI Security Standards Council

Corporate Office

295 NE Venture Drive

Waukee, IA 50263

United States

John T. Schelewitz

Regional Sales Director

ecfirst/HIPAA Academy

Phone: +1.480.663.3225

Email: John.Schelewitz@ecfirst.com

www.ecfirst.com