Composite presentation of

Disaster Recovery, Business Continuity Planning,

IT Security and Compliance

Services provided by Tom Bronack

Thomas Bronack
Phone: (718) 591-5553
Cell: (917) 673-6992
Email: bronackt@dcag.com
Mission Statement and Scope

Mission Statement:

To develop and implement Continuity of Business (COB) Plans throughout the Organization for both Business Locations (Business Continuity Planning – BCP) and Data Processing Sites (Disaster Recovery Planning - DRP).

Scope:

- Define Regulatory and Business Requirements associated with DR / BCP Plans.
- Perform a Risk Assessment to define the present state of Continuity of Business Planning.
- Identify gaps and exposures in existing BCP/DR Plans.
- Formulate methods for correcting exposures and eliminating gaps in Recovery Plans.
- Recommend a plan to implement a common BCP/DR process throughout the Company.
- Identify Internal and External personnel needed to support DR/BCP Implementation Plan.
- Establish Recovery teams and meet to define direction, objectives, needs, and timeframe.
- Create a DR/BCP project plan and gain management approval.
- Provide training to all team personnel so that everybody is aware of direction and they have an opportunity to raise concerns associated with the plan.
- Commence work on project plan and conduct periodic status meetings to ensure adherence to plan and timeframe.
Why you need a Recovery Plan

* Justifying the Need for a Recovery Plan.
  - Enterprise-Wide Commitment
  - Disaster and Business Recovery Planning implementation.
  - Risk Management implementation.

* Laws and Regulators.
  - Controller of the Currency (OCC).
    - OCC-177 Contingency Recovery Plan.
    - OCC-229 Access Controls.
    - OCC-226 End-User computing.
    - Sarbanes-Oxley, Gramm-Leach-Bliley,
    - HIPAA, The Patriot Act, etc.

* Penalties.
  - Three Times the Cost of the Outage.
  - Jail Time is possible.

* Insurance.
  - Business Interruption Insurance.
  - Directors and Managers Insurance.

“For Contingency Planning to be successful, a company-wide commitment, at all levels of personnel, must be established and funded. Its purpose is to protect the company, its business, its shareholders, and its employees.”

“Define all Regulatory, Legal, Financial, and Industry rules and regulations that must be complied with, and assign the Risk Manager with the duty of insuring that these exposures are not violated”.

“Have the Legal and Auditing Departments define the extent of Risk and Liabilities, in terms of potential and real Civil and Criminal damages that may be incurred.”.

“Once you have defined your exposures, construct an insurance portfolio that protects the business from sudden damages that could result from a disaster event.”
Business Continuity Planning Laws and Regulations

Federal Trade Commission (FTC):

- GLB Privacy Rule – requires a written information security program and protection over customer data.

Department of Health and Human Services (DHHS):

- Final Security Regulations under HIPAA (“Security Rule” - comply by 4/2005) covering Electronic Protected Health Information. Responsible for: ensuring the integrity, confidentiality and availability of EPHI; protect EPHI against reasonably anticipated threats or hazards to its security or integrity and unauthorized use or disclosure.
- HIPAA (effective 4/2003) regulates all types of health information, including paper records.

Securities and Exchange Commission (SEC):

- Final rules for Section 404 of the Sarbanes-Oxley Act of 2002 to be effective 6/2004 for all SEC reporting companies. The 404 Rules require CEOs and CFOs to provide written report on state of data security and ability to recover from disaster event.

Non-Compliance:

- Can result in criminal and/or civil damages; liability and criminal prosecution for responsible companies and individuals.
- Although the rules stress the protection, preservation and retention of records and data, their principal purpose is the establishment of a control environment that will govern how transactions are to be carried out, recorded and reported in accordance with management’s authorization and applicable policies and procedures.
- Additional losses include; reputation, trust, and general enterprise value.
- Go to www.erm.coso.org for details relating to Committee of Sponsoring Organizations (COSO) industry standards relating to Enterprise Risk Management (ERM). Documents can be downloaded.
<table>
<thead>
<tr>
<th>Covered Entities</th>
<th>Effective Date:</th>
<th>Compliance Deadline</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Institutions as defined in the Bank Holding Company Act that possess, process, or transmit private customer information.</td>
<td>May 23, 2002</td>
<td>May 23, 2003</td>
<td>Protect Customer Information from unauthorized disclosure or use.</td>
</tr>
<tr>
<td>Organizations that possess, transmit, or process electronic protected health information (EPHI).</td>
<td>April 21, 2003</td>
<td>April 21, 2005</td>
<td>Protect EPHI from unauthorized disclosure or use.</td>
</tr>
<tr>
<td>Publicly owned companies that file periodic reports with the SEC.</td>
<td>June 5, 2003</td>
<td>June 15, 2004 (for public companies with market cap. of $75 million or more)</td>
<td>Provide senior management assessment of effectiveness of company’s “internal controls for financial reporting” and attestation by independent auditors.</td>
</tr>
<tr>
<td>Any public or private entity that has unencrypted electronic personal information of California residents.</td>
<td>July 1, 2003</td>
<td>June 15, 2005 (for other SEC reporting companies)</td>
<td>Protect California residents from Identity Theft.</td>
</tr>
</tbody>
</table>

### Existing Laws and their Consequences

<table>
<thead>
<tr>
<th>Operative Mechanisms</th>
<th>Criminal Consequences of Noncompliance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information Security Program:</strong></td>
<td><strong>Fines and Imprisonment for up to 5 years.</strong></td>
</tr>
<tr>
<td>• Responsible Employee Selection,</td>
<td><strong>Fines to $250,000 and imprisonment for up to 10 years.</strong></td>
</tr>
<tr>
<td>• Risk Assessment,</td>
<td><strong>Fines up to $5 million and prison sentences for up to 20 years for deliberate violations.</strong></td>
</tr>
<tr>
<td>• Information Safeguards and Controls,</td>
<td><strong>Civil liability to any injured California resident.</strong></td>
</tr>
<tr>
<td>• Oversight of “Service Providers”,</td>
<td><strong>Internal Control Framework:</strong></td>
</tr>
<tr>
<td>• Testing and Monitoring.</td>
<td>• (Coso Framework or Equivalent)</td>
</tr>
<tr>
<td><strong>Security Safeguards:</strong></td>
<td>• Control environments – Compliance and Ethics,</td>
</tr>
<tr>
<td>• Risk Assessment,</td>
<td>• Risk Assessment and Analysis,</td>
</tr>
<tr>
<td>• Policies and Procedures to control access,</td>
<td>• Control Activities – policies, procedures, controls,</td>
</tr>
<tr>
<td>• Physical Security Measures,</td>
<td>• Information and Communications,</td>
</tr>
<tr>
<td>• Contingency Plan,</td>
<td>• Monitoring or operations and control activities to determine ongoing effectiveness of internal controls.</td>
</tr>
<tr>
<td>• Appointment of Security Officer,</td>
<td>• Testing and Evaluation.</td>
</tr>
<tr>
<td>• Training and communication to increase awareness,</td>
<td><strong>Criminal Consequences of Noncompliance:</strong></td>
</tr>
<tr>
<td>• Audits and maintenance of Audit Trails,</td>
<td>• Agreements with “business associates”,</td>
</tr>
<tr>
<td>• Agreements with “business associates”,</td>
<td>• Testing and Evaluation.</td>
</tr>
<tr>
<td>• Testing and Evaluation.</td>
<td><strong>Purpose:</strong></td>
</tr>
<tr>
<td><strong>Operative Mechanisms</strong></td>
<td><strong>Protect Customer Information from unauthorized disclosure or use.</strong></td>
</tr>
<tr>
<td><strong>Existing Laws and their Consequences</strong></td>
<td><strong>Protect EPHI from unauthorized disclosure or use.</strong></td>
</tr>
<tr>
<td><strong>Compliance Deadline</strong></td>
<td><strong>Provide senior management assessment of effectiveness of company’s “internal controls for financial reporting” and attestation by independent auditors.</strong></td>
</tr>
<tr>
<td><strong>Effective Date:</strong></td>
<td><strong>Protect California residents from Identity Theft.</strong></td>
</tr>
</tbody>
</table>

---

**Protected Health Information (PHI):**

- Includes medical records, treatment information, and billing data.
- Subject to the Health Insurance Portability and Accountability Act (HIPAA).

**Criminal Consequences of Noncompliance:**

- Fines and imprisonment for up to 5 years.
- Fines to $250,000 and imprisonment for up to 10 years.
- Fines up to $5 million and prison sentences for up to 20 years for deliberate violations.

**Civil Consequences:**

- Civil liability to any injured California resident.
Corporate and Departmental Responsibilities

**Corporate Responsibilities**

**Security** Department for building access, Police, Fire, and Emergency Medical.

**Facilities** for Salvage & Restoration.

**Personnel** for casualties and First Aid Training.

**Public Relations** for statements to Press and other types of Media.

**Purchasing** for equipment acquisition.

**Administration** for office supplies and coordination of logistics and Essential Services / Suppliers.

**Leasing** to obtain equipment.

**Legal and Audit** departments to insure compliance to regulatory requirements.

**Audit** to review recovery plans for compliance to business needs.

**Recovery Planning**

Define **Recovery Sections** to be completed by Corporation and individual **Departments**.

Define **Disaster Recovery Manual** sections, their format and content.

Establish **Contingency Recovery Organizational** Structure.

Formulate **Disaster Recovery Teams**.

**Create** Disaster Recovery Plans.

**Test and Implement** Disaster Recovery Plans.

Formulate **Disaster Definition and Declaration** procedures.

**Coordinate** disaster event to Disaster Team activation process.

** Maintain** Disaster Recovery Plans.

**Recovery Sites**

**Contingency Command Center** - Small to Large, in relationship with scope of disaster event.

**Data Center Recovery Site**

**Office Recovery Site**

**Problem Management**

**Problem** definition and escalation procedures.

**Change Management** for New and Altered applications and environments.

**Help Desk** procedures and scripts to address problem events, with escalation process in place for declaring disasters and activating Disaster Teams.
Contingency Planning

Contingency Recovery Disciplines

Charter:
1. Eliminate Business Interruptions.
2. Ensure Continuity of Business.
4. Adhere to Legal / Regulatory Requirements.

EDP Protection:
2. Data Sensitivity and Access Controls.
4. Mainframe / Mid-Range disaster recovery.

Corporate Asset Protection:
1. Inventory Control.
2. Asset Management.
3. Configuration Management.
5. Office Recovery.

Management Controls:
1. Exposures.
2. Insurance.
3. Legal / Regulatory Requirements.
5. Vendor Agreements.

“Contingency Planning affects every part of the organization and is separated into logical work areas along lines of responsibility.”

“Establishing interfaces with key departments will allow for the inclusion of corporate-wide recovery procedures (Security, Salvage, and Restoration, etc.) in department specific Recovery Plans.”

Contingency Recovery Interfaces

Executive Management
Data Processing
Company Operations
Auditing
Public Relations
General Services
Personnel
Facilities

Contingency Recovery Planning
The “Ten Step” Process

Recommended by the Business Continuity Institute for BCP (see: www.thebci.org)

1. Project Initiation and Management.
2. Risk Evaluation and Control.
5. Emergency Response and Operations.
7. Awareness and Training Programs.
Contingency Planning Strategy

(FEMA) EMERGENCY MANAGEMENT PREPAREDNESS – PROJECT PLAN

THE PLANNING PROCESS:
1. Establish a Planning Team.
2. Analyze Capabilities and Hazards.
3. Develop the Plan.
4. Implement the Plan.

HAZARD SPECIFIC INFORMATION:
1. Fire.
3. Floods and Flash Floods.
4. Tornadoes.
5. Severe Winter Storms.

EMERGENCY MANAGEMENT CONSIDERATIONS:
1. Direction and Control.
2. Communications.
3. Life Safety
4. Property Protection.
5. Community Outreach.
7. Administration and Logistics.

APPENDICES:
1. Vulnerability Analysis Chart.
2. Training Drills and Exercises Chart.
3. Information Sources (where to turn For additional information).
Getting Started

• Strong Management Backing and Commitment.
  • Compliance, Industry, and Business Regulatory Requirements.

• Contingency Planning Organization:
  • Contingency Recovery Interfaces.
  • Systems Management Disciplines.
  • Component and Release Management.
  • Problem Management Overview.
  • Project Management, Goals, and Deliverables.
  • Business Recovery Planning.
  • Vital Records Management Personnel Functions.
  • Integrating DR and BCP Plans within Command Center.
  • Informational Requirements and Workflow Process Integration.
  • Standards and Procedures.
  • Awareness and Educational Training.

• Risk Assessment and Business Impact Analysis (BIA).

• Contingency Plan Creation, Testing and Implementation.

• Contingency Planning Support and Maintenance.
COSO Risk Assessment

Committee Of Sponsoring Organizations (COSO) was formed to develop Risk Management and Mitigation Guidelines throughout the industry.

Designed to protect Stakeholders from uncertainty and associated risk that could erode value.

A Risk Assessment in accordance with the COSO Enterprise Risk Management Framework, consists of (see www.erm.coso.org for details):

- Internal Environment Review,
- Objective Setting,
- Event Identification,
- Risk Assessment,
- Risk Response,
- Control Activities,
- Information and Communication,
- Monitoring and Reporting.


Implementation of Standards and Procedures guidelines associated with Risk Assessment to guaranty compliance to laws and regulations.

Employee awareness training, support, and maintenance going forward.
Performing a Risk Assessment or Needs Analysis

I. PERFORMING A RISK ASSESSMENT:

A. Define Laws and Regulatory Requirements.
   1. Gramm-Leach-Bliley,
   2. Sarbanes-Oxley,
   3. HIPAA,
   4. Patriot Act,
   5. EPA and Superfund,
   6. Industry Specific Regulators.

B. General Recovery Parameters:
   1. Data Sources and their Protection,
   2. Business Continuity Planning,
   3. Library / Vital Records Management,
   4. Disaster Recovery Planning,

C. Define Business / Disaster Recovery Needs:
   1. Define Business Continuity Needs,
   2. Implement IT & Physical Security,
   3. Implement Vital Records and Library Management,
   4. Develop Disaster Recovery Planning,
   5. Implement Recovery Operations,
   6. Support and Maintain Recovery Plans,
   7. Insure Protection of Business Assets,
   8. Assure Regulatory Compliance,
   9. Assure Insurance requirements are met.
   10. Assure Vendor Contracts and Reciprocal Agreements are in place and maintained.
   11. Develop Recovery Plan(s), as per existing Standards and Procedures.
   12. Monitor Recovery Test(s) and Post Mortem meetings.
Disaster Recovery Plan Data Sources and Output Generation

- Equipment
- Facilities
- Forms
- Software
- Supplies

- Vital Records
- Recovery Tasks

- Form Screen and Merge Data

- Disaster Recovery Database

- Mail-Merge Product

- Extract, Merge, Tailor, and Report

- Mail Merge

- Disaster Recovery Templates

- Word Templates

- Disaster Recovery Plans
- Disaster Recovery Plans

Data Center Assistance Group, Inc.  Composite presentation on Disaster Recovery  Page: 13
Overview of Business Continuity Planning and BIA’s

Recovery Plans direct personnel to restore business operations in response to encountered problems. The Help Desk escalates critical problems, initiates recovery plans, and manages recovery activities.
Contingency Command Center:

- Housed within Command Center,
- Activated during Emergencies,
- Relates problems to Recovery Plan,
- Activates appropriate Recovery Team(s),
- Coordinates Recovery Actions,
- Maintains status on disaster and crisis situations,
- Communicates with:
  - Network Control Center,
  - Operations Control Center,
  - Help Desk,
  - Technical Staff, and
  - Management.
- Will escalate recovery actions, if necessary.
Strategies for Eliminating Audit Exceptions

• Review of Compliance Requirements (Business and Industry)
• Data Sensitivity, EDP Security and Vital Records Management,
• Production Acceptance, Quality Control and Project Life Cycle,
• Utilizing Automated Tools,
• Elimination of Single-Point-Of-Failure concerns,
• Inventory / Asset Management,
• Problem and Crisis Management,
• Work-Flow automation through Re-Engineering processes,
• Training and Awareness programs.
Systems Management Organization

- Service Level Management
- Inventory & Asset Management
- Configuration Management
- Capacity Management
- Performance Management
- Application Development (PLC)
- Application Maintenance
- Application Testing
- Quality Assurance
- Production Acceptance
- Production Operations
- Change Management
- Problem Management
- Contingency Management
- EDP Security Management
- Vital Records Management
- Business Recovery
- Risk Management
- Disaster Management

Data Center Assistance Group, Inc. Composite presentation on Disaster Recovery Page: 17
Systems Management Controls and Workflow

Service Level Reporting, Capacity Management, Performance Management, Problem Management, Inventory Management, Configuration Management.

- Development
  - Service Level Management, Project Life Cycle,

- Testing
  - Quality Assurance
    - Test Validation, Components, Naming, Placement, Functionality, Process.

- Production Acceptance
  - Production
    - Batch and On-Line Management

- Maintenance
  - Change Management
    - Project Life Cycle, Component & Release Management, Standards & Procedures, User Guides & Vendor Manuals, Training (CBT & Classroom), etc...

- Disaster Recovery
  - Off-Site Vault
    - Disaster Recovery Facility
      - Mainframe and Office Recovery

Vital Records

A Forms Management & Control System, used to originate work requests and track work until completed, will facilitate optimum staff productivity and efficiency.
Application Life Cycles and Business Recovery Planning

*Development through Change Management and Maintenance*

**Development**
- End User Request for new program
- On-Line data files

**Testing**
- Unit & System Testing
- BKUP

**Quality Assurance**
- JCL, Naming, Placement

**Production Acceptance**
- BKUP
- On-Line data files

**Development Through Change Management and Maintenance**

**Maintenance**
- Enhance and Repair

**Change Management**
- Release and Version Control

**Production**
- BKUP
- On-Line data files

**End-User Location**
- New

**End-User defines:**
- Business Purpose,
- Business Data,
- Ownership,
- Sensitivity,
- Criticality,
- Usage,
- Restrictions,
- Back-Up, and Restoration.

**Vendor**
- Business Recovery Facility
- Disaster Recovery Facility
- Off-Site Vault
- Update
- Recovery

**On-Line Production**
- Real-Time
- Periodic

End User defines:
- Business Purpose,
- Business Data,
- Ownership,
- Sensitivity,
- Criticality,
- Usage,
- Restrictions,
- Back-Up, and Restoration.

Data Center Assistance Group, Inc.
Composite presentation on Disaster Recovery
Page: 19
Interfaces Between Applications, QA, and Production Groups.

### APPLICATIONS GROUP

1. Create Service Request
2. Perform Technical Assessment
3. Perform Business Assessment
4. Perform Requested Work
5. Application Group Testing

Error Loop

- CP #1
- No
- Successful

If Successful, then:
- Create QA Turnover Package

If Not Successful, then:
- Return to Submitter

### QA GROUP

1. Perform Post-Mortem
2. Perform Requested Work
3. QA Review Meeting
4. Schedule Request
5. QA Review and Accept

Error Loop

- CP #2
- No
- CP #3

- Successful

If Successful, then:
- Perform User Acceptance Testing

If Not Successful, then:
- Proceed with Error Loop

### TESTING and QA

Turnover Package Components:
- Service Form and results Assessments,
- Change & Release Notes,
- Application Group Testing Results,
- Test Scenarios & Scripts,
- Messages & Codes, and Recoveries,
- Data for Regression and Normal Testing,
- Documentation.

### PRODUCTION CONTROL

Turnover Package Components:
- Explanation and Narrative,
- Files to be released,
- Predecessor Scheduling,
- Special Instructions,
- Risk Analysis,
- Authorizations.
Problem Management Techniques

Users
NCC
OCC
HD

Problem

Symptoms
Analyze
Circumvent
Document
Log Problem
Route / Escalate
Track
Resolve
Post Mortem
Upgrade Supportive Documentation

Immediate actions

Follow-on Actions

Problem Indicators
Console Log
Completion Code
Unexpected Results

Problem Descriptions
Meaning
Possible Causes
Actions to be Taken

Problem Bypass Procedures
Recovery Procedures
Restart Procedures

Problem History

Problem Record

Problem Repository

Problem Feed-Back, Rerouting and Escalation

Problem Resolvers

1 System Software
2 Comm. Systems
3 Corp. Security
4 DB Systems
5 DASD
6 Cap. & Performance
7 Decision Support
8 Optical Storage
9 CICS
10 Systems Mgmnt. and Controls

Diagnostic Tools
Omegamon
AF / Operator
Netview
OPC / ESA

Reference Materials
Messages and Codes
Job Runbook

Job Runbooks
S&P Manual
User Guides
Inventory & Configuration

Problem History

Review Problem Reporting and Resolution Procedures

Immediate actions

Follow-on Actions

Problem Feed-Back, Rerouting and Escalation

Diagnostic Tools
Omegamon
AF / Operator
Netview
OPC / ESA

Reference Materials
Messages and Codes
Job Runbook

Job Runbooks
S&P Manual
User Guides
Inventory & Configuration

Problem Resolvers

1 System Software
2 Comm. Systems
3 Corp. Security
4 DB Systems
5 DASD
6 Cap. & Performance
7 Decision Support
8 Optical Storage
9 CICS
10 Systems Mgmnt. and Controls

Data Center Assistance Group, Inc. Composite presentation on Disaster Recovery Page: 21
Contingency Organization in Action

Contingency Command Center

Contingency Recovery Coordinator

Situation Manager

Help Desk

"Critical Problems, or Disaster Events"

Problem Matrix

Contingency Recovery Team
Contingency Recovery Team
Contingency Recovery Team
Contingency Recovery Team

Operations
Systems
Communications
Applications

Operations Analyst
Technical Support Staff
Communications Support Analyst
Applications Support Staff
Contingency Recovery Operations

Contingency Recovery Coordinator

Responds to problems classified as “Potential Crisis Situations” by:

- Logging the problem within the Problem Log;
- Comparing the problem to the Recovery Matrix;
- Selecting the appropriate Recovery Plan;
- Activating the Recovery Team identified within the Recovery Plan; and,
- Monitoring recovery operations and reporting on their status to Management.

Situation Manager

Reporting to the Contingency Recovery Coordinator and responsible for monitoring Recovery Team operations and providing assistance through any mechanism at their disposal. When situations become overly complex and a potential crisis can occur, the Situation Manager will take appropriate escalation procedures needed to concentrate more resources on the resolution of the problem.

Recovery Teams

Designed to pull expertise together so that specific talents can address problems that require recovery operations, before normal processing can be resumed. Each Recovery Team consists of a Team Manager and Team Members. The organization of a Recovery Team is supplied to the Situation Manager and Contingency Recovery Coordinator. This organizational description includes functional responsibilities and alternate personnel for each of the recovery positions. Recovery Teams may require recovery tools to be utilized as an aid in performing recovery operations.
Business Recovery Services

- **Risk Assessment** to identify Continuity of Business (COB) exposures and gaps relating to newly adopted COB requirements.
- **Business Impact Analysis** requirements definition and risk analysis studies,
- **Data Sensitivity** studies and evaluations,
- **EDP Security** (**Physical and Data**) studies and evaluations,
- **Vital Records** (**Vaulting Services**) and/or **Library Management**,
- **Business Recovery Documentation** evaluation and needs definition,
- **Business Recovery Plan** (**Development, and/or Implementation**),
- **Disaster Recovery Vendor(s)** (**Evaluations through Selection**),
- **Business Recovery Training**, 
- **Permanent Personnel Recruitment and Placement Services**, 
- **Consulting and Temporary Personnel Services**.
Overview of our Services
(Part 1 of 3)

We provide Consulting and Personnel Placement Services, along with providing Compliance Services to assist clients adhere to the regulatory requirements of the laws listed below. These services make our firm unique.

We provide Consulting and Personnel Placement Services, along with providing Compliance Services to assist clients adhere to the regulatory requirements of the laws listed below. These services make our firm unique.

• Project Definition & Scope
• Goals and Objectives
• Team identification
• Team Assignment
• Team Training
• Project Plan Creation
• Project Management & Status Reporting
• Analysis Phase
• Conclusions
• Recommendations
• Management Report
• Management Presentation

• COSO Format, including:
  • Internal Environment,
  • Objective Setting,
  • Event Identification,
  • Risk Assessment,
  • Risk Responses,
  • Control Activities,
  • Information and Communications

  • Monitoring and Reporting.
  • Management Report
  • Management Presentation

• Physical Security, including:
  • Perimeter,
  • Access Controls,
  • Surveillance & Reporting,
  • Fire Safety Protection.

• IT Security, including:
  • Data Sensitivity,
  • Access Controls,
  • Vital Records,

  • Backup & Restoration.
  • Data Management Tools.

• Disaster Recovery,
• Emergency Management,
• Business Impact Analysis,
• Contingency Command Center,
• Documentation,
• Team Selection,
• Team Training,
• Support,
• Maintenance.

• Organizational Structure,
• Systems Management,
• Job Descriptions,
• Functional Responsibilities,
• Forms Management,
• SLA / SLR,
• Standards & Procedures,
• Personnel Training.
Overview of our Compliance Services  
(Part 2 of 3)

Services

Consulting
- Sarbanes Oxley
  - All Public Companies over $75 Million in Revenue:
    - Sections 302, 404, and 409
    - Risk Assessment
    - Checks & Balances
    - IT Security
    - Systems Development
    - Life Cycle
    - Systems Management
    - Recovery
    - Standards & Procedures
    - Documentation & Training
    - Support
    - Maintenance

- Gramm Leach Bliley
  - All Financial Organizations that possess, process, or transmit private customer data:
    - Risk Assessment
    - Responsible Employee Selection
    - IT Security
    - Oversight of “Service Providers”
    - Testing and Monitoring
    - Evaluation & Reporting to management
    - Standards & Procedures

- HIPAA
  - All Companies that possess, process, or transmit Electronic Protected Health Information:
    - Risk Assessment
    - Standards & Procedures
    - IT Security
    - BCP and DR Planning
    - Security Officer & BCP Officer
    - Documentation & Training
    - Periodic Audits
    - Agreement with Business associates to adhere to policies
    - Ongoing Testing & Maintenance

- The Patriot Act
  - Terrorism Act to protect Americans from attack:
    - Risk Assessment
    - Customer Screening Procedures
    - Customer Information Program (CIP)
    - Protecting Confidentiality, while aiding investigations
    - Foreign Intelligence Investigations
    - Money Laundering
    - Standards & Procedures
    - Documentation & Training

- EPA / Superfund
  - Protecting the environment and cleaning up landfills:
    - Risk Assessment
    - Toxic Materials
    - Protect Employees
    - Protect people in area
    - Waste Removal Procedures
    - Standards & Procedures
    - Documentation & Training
    - Support & Maintenance

Data Center Assistance Group, Inc.  Composite presentation on Disaster Recovery  Page: 26
Overview of our Services  (Part 3 of 3)

Services

- Consulting
  - Permanent Staff

- Compliance
  - Temporary Staff

- Placement
  - Consultants
  - Automated Systems

- Personnel Productivity,
- Automated Personnel,
- Workflow Management,
- Automated Training.
Sarbanes-Oxley Act

- Requires companies to perform quarterly self-assessments of risks to business processes that affect financial reporting and to attest to findings on an annual basis (CFO and CEO, possibly CIO too). Section 302 requires “Signing Officer” to design reports for compliance submission.

- Section 404 requires that technology personnel develop and implement means for protecting critical financial data (data security, back-up and recovery, business continuity planning, and disaster recovery), because loss of data is not acceptable.

- Section 409 will require “Real-Time Reporting” of financial data, thus creating the need for new Standards and Procedures and perhaps re-engineering of functions to better comply with the Law.

- Companies must devise “Checks and Balances” to guaranty that those people creating functions (like programmers) are not the person responsible for validating the functions operation (rather a separate checker must validate function).

- Checks and Balances prohibit big 4 accounting firms from performing Risk Assessment because they are the ones performing audit (Conflict of Interest).

- Penalties can include fines as high as $5 million and imprisonment can be for as long as 20 years for deliberate violation.
Gramm-Leach-Bliley

• Covers Financial Organizations (as defined in the Bank Holding Act) that possess, process, or transmit private customer information.

• Its purpose is to protect Customer Information from unauthorized disclosure or use.

• An Information Security Program must be in place to comply and the following operating mechanisms must be established:
  – Responsible employee as Security Officer.
  – Risk Assessment to uncover and correct exposures.
  – Information Safeguards and Controls must be established.
  – Oversight of “Service Providers and Vendors” to guaranty compliance.
  – Testing and Monitoring in an on-going fashion.
  – Evaluation and Reporting to management.

• Compliance date of May, 2003. Law provides for fines and imprisonment of up to 5 years for intentional violations.
HIPAA

- **Covers** organizations that possess, transmit, or process electronic protected health information (EPHI).

- **Responsible for protecting EPHI data** from unauthorized disclosure or use.

- **Required Security Safeguards include:**
  - **Risk Assessment** to uncover and resolve exposures.
  - **Policies and Procedures** to control access and track usage.
  - **Physical and IT Security Measures.**
  - **Contingency Plan and Disaster Recovery Plan.**
  - **Appointment of Security Officer and Business Continuity Officer.**
  - **Training** and communications to improve awareness.
  - **Periodic Audits** and maintenance of Audit Trail.
  - Agreement with “**Business Associates**” to comply to requirements.
  - **On-going Testing and Evaluation of plan and deliverables.**

- **Comply by April 2005, with fines to $250,000 and imprisonment for up to 10 years.**
Patriots Act

- **New Requirements — Severe Penalties** (Official Title is “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism”).

- **USA PATRIOT Act Section 326** imposes new requirements on how organizations screen existing customers and process new customer information.

- **By October 1, 2003**, all financial services organizations must have in place procedures for:
  - 1. **Customer Screening** — On a regular basis, customers and transactions must be matched against government-provided lists of suspected terrorists, drug traffickers, money launderers and other criminals.
  - 2. **Customer Information Program (CIP)** — On all new customers, basic identification information must be obtained to verify the customer's identity. Failure to comply can result in penalties of up to $1 million, and/or imprisonment.

- Used to **protect the confidentiality** of telephone, face-to-face, and computer communications, **while enabling authorities to identify and intercept during criminal investigations** with warrant.

- Improves ability to obtain data during **Foreign Intelligence Investigations** and increases a companies need to safeguard voice, face-to-face, and computer based data.

- Enhances financial organizations ability to track suspected **Money Laundering** activities and requires reporting of activity when uncovered, thus fostering the need to obtain, store, and safeguard data used to report on suspected Money Laundering activities.
EPA and Superfund

• Designed to **protect the environment** from Toxic Materials that could lead to death or illness.

• **Regulated** by the Environmental Protection Agency.

• **Fines and imprisonment** can be imposed when violation is intentional, or through a third party acting in your behalf.

• **Safeguards** should be imposed to:
  – **Identify** toxic materials,
  – Take appropriate steps to **protect** employees and community personnel,
  – Insure that proper and authorized **Waste Removal procedures** are implemented,
  – **Provide personnel awareness programs and Standards and Procedures**,
  – **Support and maintain** program going forward.
Creating Compliance Reports

Sarbanes Oxley Act (SOA) (Enacted)

Section 302
Design Compliance Reports

Section 404
Manual Compliance Reporting

Section 409
Automated Compliance Reporting

Sarbanes Oxley Act (SOX) Reporting

Signing Officer(s)
CEO, CFO and Compliance Officer

Review Compliance Requirements

Design Compliance Reports

Re-Design Compliance Reports

Agree on Reports?

No

Yes

Create (TRM) Technical Risk Manager

Create (ORM) Operational Risk Manager

Depts. Extract Reporting Data (Manual Mix)

CEO / CFO Attest To Compliance

OK?

N

Y

CEO and CFO Review Report(s)

ORM Report(s) Review

TRM Report(s) Review

ORM Review

TRM Review

Reports Submitted

CEO and CFO Review

Compliance Reports Created

Report(s)

Y

N

Compliance Data Extracted Automatically

Compliance Reports Generated

Re-Design Compliance Reports

Agree on Reports?

No

Yes

ORM Report(s) Review

TRM Report(s) Review

CEO and CFO Review

ORM Review

TRM Review

Reports Submitted
Section 404 of the Sarbanes-Oxley Act (SOX) says that publicly traded companies must establish, document, and maintain internal controls and procedures for Financial and Compliance reporting. It also requires companies to check the effectiveness of internal controls and procedures for Financial and Compliance reporting.

In order to do this, companies must:

- Document existing controls and procedures that relate to financial reporting.
- Test their effectiveness.
- Report on any gaps or poorly documented areas.
- Repair deficiencies and update any Standards and Procedures associated with the defects.
How do we comply?

Laws and Regulations concentrate on the VALIDITY of PROVIDED DATA, so we start with a review of how sensitive data is created, protected, and used, including:

- Identify the lifecycle of data used in financial reporting and compliance.
  - Where does it come from?
  - What form is it in (Excel, Database, manual, fax, email, etc.)
  - Who has access to it and how can they impact data (create, edit, use, convert, etc.)
- Review current Data Sensitivity and IT Security procedures.
- Examine Library Management, Backup, Recovery, and Vaulting procedures associated with sensitive data.
- Review Business Continuity Planning and Disaster Recovery procedures used to protect and safeguard critical data and facilities.
- Utilize existing Standards and Procedures to duplicate process and identify errors.
- Examine the available Employee Awareness and Education programs.

As a result of this study, it will be possible to identify weaknesses and develop procedures to overcome the weaknesses, thereby improving efficiency and productivity.
DCAG Project Phases (part 1 of 2)

Start

I
Risk Assessment
- CEO, CFO Design Reports (Section 302)
- Review and Approve Reports
- Operational Risk Manager (ORM)
- Technical Risk Manager (TRM)

II
IT Security
- Data Sensitivity Study
- Access Controls (Userid / Pswd)
- Version & Release Management
- Backup & Recovery

III
SDLC
- Development And Maintenance
- Testing and Quality Assurance
- Production Acceptance
- Production Operations
- Vital Records Management

IV
Systems Management
- SLA / SLR
- Asset Management
- Configuration Management
- Inventory Management
- Change Management
- Problem Management
- Performance Management
- Capacity Management
DCAG Project Phases (part 2 of 2)

A

V

Recovery

Business Continuity Planning
Disaster Recovery Planning
Risk Management
Contingency Planning

VI

Standards & Procedures

Standards Definition
Procedures Creation
Documentation
Forms Management & Control

VII

On-going Support

Section 404 Compliance
Section 409 Compliance
Training

End