Supply Chains and Small Business
One Aspect of the Small Business Challenge

- Maximum Tolerable Period of Disruption (MTPod)
- Recovery Point Objective
- Management Systems
- Recovery Time Objective
- Business Impact Analysis (BIA)
- Guidance Document
- Major and Minor Non-Conformance
Preparedness - 3rd Wave Imperative
1st Wave: 1850 to 1975

Market-Driven, Process Improvements

- Focus on Cost and Volume
- Theory “X” Management
- Assembly Lines
- Trade Unions
- Wealth came from “raw materials” and production facilities
The 2nd Wave Began In 1975

Market-Driven *Product* Improvements

- Cost and Volume is assumed
- Theory “Y” Management
- Quality Circles
- Shift to Low Cost Labor Sites
- Development of Outsourcing
- Wealth comes from Process “Know-How”
Now the 3rd Wave

- In the United States and Europe, supply chains are 4 to 7 layers deep (Farm to Fork)
- Some are dozens deep.
Can You Be Depended On?

- Cost & Volume is Assumed
- Quality is Assumed
- Regulation is Increasing
- Shift to Reliable Sites
• Huge Financial Impact
According to the Brookings Institute, 15% of the value of an enterprise resides in tangible assets, while 85% rests in intangible assets - the largest part of those intangibles being information.
A Stair-step Approach to Preparedness

Focus on education and incremental development
A Mentoring Role: 2\textsuperscript{nd} Party Assessments
Dealing with Executive Resistance?
Evolution of Justification Argument - General

- **Stage 1**: Unclear Use
  - Soft $
  - Education
  - Entertainment

- **Stage 2**: Targeted Use
  - Hard $
  - “Killer App” Concept

- **Stage 3**: Operational Integration
  - Obvious Value
  - Reuse
  - Re-purpose

- **Stage 4**: Embedded Capability
  - Ubiquitous (None Needed)
  - Culture Shift

- **How used**
  - Non-Specific
  - Identified Use
  - General Operations

- **Argument Type**
  - Soft $ → Hard $ → Obvious Value → Ubiquitous
  - Soft $ → Hard $ → Obvious Value → Ubiquitous
  - Soft $ → Hard $ → Obvious Value → Ubiquitous
  - Soft $ → Hard $ → Obvious Value → Ubiquitous
Example 1: The Telephone

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>How Used</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>General Operations</td>
</tr>
<tr>
<td></td>
<td>Identified Use</td>
</tr>
<tr>
<td></td>
<td>Non-Specific</td>
</tr>
<tr>
<td>Soft $</td>
<td>Limited Use</td>
</tr>
<tr>
<td>Hard $</td>
<td>Market Penetration</td>
</tr>
<tr>
<td>Obvious Value</td>
<td>Business Tool</td>
</tr>
<tr>
<td>Ubiquitous</td>
<td>Multi-functional</td>
</tr>
<tr>
<td></td>
<td>Indispensable</td>
</tr>
<tr>
<td>Culture Shift</td>
<td></td>
</tr>
</tbody>
</table>

*Soft $* refers to costs associated with the implementation and use of the telephone.

*Hard $* refers to the tangible benefits and returns on investment.

*Obvious Value* indicates the clear and immediate benefits of the telephone to businesses.

*Ubiquitous (None Needed)* signifies the widespread adoption and integration of the telephone into daily operations.
Example 2: The PC

The "Killer App": Spreadsheets, Word Processing, Others

The Internet

Fabric of Society

Culture Shift

General Operations

How Used

Identified Use

Non-Specific

Soft $

Hard $

Obvious Value

Ubiquitous (None Needed)

Argument Type

Entertainment & Education
Small and Large Business Preparedness

- **Soft $**: Non-Specific, Optional Commitment
- **Hard $**: Identified Use, Committed Resources, Dedicated Technology
- **Obvious Value**: Budgeted Line Item
- **Ubiquitous (None Needed)**: Operationally Pervasive, Culture Shift

**Argument Type**

**How Used**

- **General Operations**
- **Identified Use**
- **Non-Specific**
How Soon?

The works of two authors

Malcolm Gladwell: *The Tipping Point*

Geoffrey A. Moore: *Crossing the Chasm*
Supply Chain Leads the Way
The Other Arguments

– Governance
– Valuation
– Compliance
– Risk Management
– Liability
– Supply Chain

Part of the necessary evolution of Public-Private collaboration and executive acceptance of the value of preparedness.
Making Progress, But More to Do!
The Small Business Challenge
The Mechanics of ISO Auditing
There Are 9 Types of Audits

1. Organization Registration/Certification

3 Versions
- 1st Party
- 2nd Party
- 3rd Party
3rd Party Audits consist of 2 “stages”

- Stage 1: Document Review
- Stage 2: Onsite inspection and discussions. Evidence-based
  - No claim of statistical significance can be made!
  - Some standards establish guidelines (ISO 28001)
  - PS Prep standards do not use these guidelines (ANAB decision)
- No consulting can take place!

Audit plan must be submitted in advance and agreed to by both parties. Discusses location, logistics, and process.

Management should be present for the beginning and end as well as for discussion on an “as needed” basis.

Have your paperwork ready. This is not covered in a Stage 1
The Audit Process – Stage 1
Stage 2: On-site Audits

- Executive Interviews
- Team discussions
- Survey’s
- Record inspections
  - Not Statistical Sampling
- Documentation review
- Training records
- Contracts review
- Observations
- Customer correspondence
Sample Stage 1 Report

BS 25999-2 STAGE 1 AUDIT REPORT

1. Complete the following table of locations to be included in the scope of the audit. Confirm information with the organization. DO NOT RELY ON INFORMATION INCLUDED IN THE T-Z. Note: If distinct addresses exist for adjacent buildings, this table must be listed.

<table>
<thead>
<tr>
<th>Address</th>
<th>Description of activities</th>
<th># of employees</th>
<th># of Shifts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Planning the Business Continuity Management System

2a. Has the organization defined the scope of its business continuity management system (BCM)?

   □ CONFORMS  □ NONCONFORMS  □ CONCERN

   Evidence of conformity, nonconformity, or concerns for follow-up at Stage 2: 

   Document the scope here: 

   List any exclusions here: 

   Summarize justification for organization’s exclusions here: 

2b. Has the organization identified the key products and services within the scope of its BCM?

   □ CONFORMS  □ NONCONFORMS  □ CONCERN

   Evidence of conformity, nonconformity, or concerns for follow-up at Stage 2: 

2c. Has the organization set business continuity objectives that reflect consideration of the following: requirements for business continuity, organization at objectives and constraints, acceptable level of risk, statutory, regulatory, and contractual duties and interests of key stakeholders?

   □ CONFORMS  □ NONCONFORMS  □ CONCERN

   Evidence of conformity, nonconformity, or concerns for follow-up at Stage 2: 

2d. Has the organization communicated a business continuity management policy that is consistent with the organization’s objectives?

   □ CONFORMS  □ NONCONFORMS  □ CONCERN
Opening and Closing Meetings

This is where the work really begins

Auditors will expect management to be present

They will ask for confirmation of the scope statement

Suggestion:
- Don’t volunteer to activities that are out of the plan
- Don’t let someone who is not briefed on the protocol, speak!

The auditors will follow a prescribed format
**Typical Audit Plan**

<table>
<thead>
<tr>
<th>Date</th>
<th>December 30, 2006</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Name</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Team</td>
<td></td>
</tr>
<tr>
<td>Technical Expert</td>
<td></td>
</tr>
<tr>
<td>Lead Auditor</td>
<td></td>
</tr>
<tr>
<td>Employee Count</td>
<td></td>
</tr>
<tr>
<td>Number of Visits</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Typically an audit plan will include the scope of the audit. This defines the parameters of the audit and the areas to be investigated.</td>
</tr>
<tr>
<td>Purpose</td>
<td>The purpose of the audit is to evaluate the effectiveness of the organization's policies and procedures, and to identify areas for improvement.</td>
</tr>
<tr>
<td>Method</td>
<td>The audit method should be documented and should include a description of the techniques and tools used.</td>
</tr>
</tbody>
</table>

**Reference Documents**

- ISO 9001:2015, Guidance on quality and environmental management systems auditing
- ISO 14001:2015, Guidance on environmental management systems auditing
- ISA-101:2015, Guide to automation in the process industries
- ISA-5.1.1:2001, Guide to instrument specification
- ISA-5.1.2:2001, Guide to instrument calibration
- ISA-5.1.3:2001, Guide to instrument maintenance
- ISA-5.1.4:2001, Guide to instrument troubleshooting

**Audit Language**

- Audit Working Language: English
- Audit Reporting Language: English

**Confidentiality**

- All information obtained during the audit shall be treated as confidential and shall not be disclosed to any unauthorized person(s) without the prior written consent of the audit team.

**Audit Requirements**

- Audit team members shall observe all applicable laws, regulations, and organizational policies.
- All audit findings shall be documented in a timely manner.

**Note:**

1. Auditors are responsible for maintaining the confidentiality of all information obtained during the audit.
2. Auditors are responsible for ensuring that all findings are documented in a timely manner.
3. Auditors are responsible for ensuring that all audits are conducted in accordance with the audit plan.
Audit Plan Continued
## A Typical Audit Module

<table>
<thead>
<tr>
<th>Governance</th>
<th>4.1 Leadership and Commitment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4.1.1 The entity leadership and management commitment to the program to prevent, mitigate the consequences of, prepare for, respond to, and recover from emergencies.</td>
</tr>
<tr>
<td></td>
<td>4.1.2 The leadership commitment shall include the following:</td>
</tr>
<tr>
<td></td>
<td>1) Policies, plans, and procedures to implement and maintain the program.</td>
</tr>
<tr>
<td></td>
<td>2) Resources to support the program.</td>
</tr>
<tr>
<td></td>
<td>3) Reviews and evaluations to ensure program effectiveness.</td>
</tr>
<tr>
<td></td>
<td>4) Correction of deficiencies.</td>
</tr>
<tr>
<td></td>
<td>4.1.3 The entity shall adhere to policies, execute plans, and follow procedures developed to support the program.</td>
</tr>
<tr>
<td></td>
<td>4.1.4 Leadership shall integrate with, complement and not replace policies, plans, procedures or defined responsibilities.</td>
</tr>
</tbody>
</table>

### 4.2 Program Coordinator

The program coordinator shall be appointed by the entity and authorized to administer, evaluate and maintain the program.

### 4.3 Program Committee

4.3.1 A program committee shall be established by the entity in accordance with its policy.

4.3.2 The program committee shall provide input or assist in the coordination of the preparation, implementation, evaluation, and revision of the program.

4.3.3 The program committee shall include the program coordinator and others who have the expertise, knowledge of the entity, and the capability to identify resources from all key functional areas within the entity and shall select an external or external representative.

The program committee shall have a documented program that includes the following:

1. Executive policy including vision, mission statement, roles and responsibilities, and enabling authority.
2. Program goals, objectives, and method of program evaluation.
3. Program plans and procedures to ensure the following:
   1. Anticipated cost
   2. Priorities
   3. Time to accomplishment
   4. Resources required.
4. Applicable authorities, legislation, regulations, and industry codes of practice.
Types of Findings

• Auditors have 5 options
  – **Conforms** to Standard – Goal of every audit!
  – **Minor (Partial) Non Conformance**
    • Single lapse, isolated incident, not likely to cause systemic failure
  – **Major Non Conformance**
    • Systemic breakdown
    • Pattern of failure or breakdown of policy/procedure
    • Absence of a required or necessary control/procedure/policy
  – **Observation** – comment on out of scope item (rare)
  – **Not Applicable** – asked to comment on an out of scope item
Audit Evidence

• Identify appropriate sources of information

• Collect/review an *appropriate* amount of information
  – This *is not* a statistically significant sampling exercise
  – Evidence may be gathered in many ways
    • Interviews
    • Records, including meeting minutes, sign-in sheets, copies of presentation material, post-meeting follow-up notes, emails, copies of contracts (esp. if SLA are involved), etc.
    • Team/Department meetings and discussions
    • Observations

• The goal is not to find problems, but indications and patterns
Audit Details

- Occasionally, auditors may ask for a chance to “huddle.” Please provide a private location for this.

- Auditee can also call for a “time out” to review issues and discuss performance of the audit team.

- At the closing meeting each day, ask for a detailed progress report.

- Make sure there is sufficient time at the closing meeting to get clarification on all findings.

- Stay on top of the auditor to deliver written findings in a timely and professional manner.
Appendix 6 - Summary review by UKAS technical expert

**Overall Observations**

1. There is a clear mismatch between what the BCPG director and auditors see what the BCPG 2 and BCM owners think the situation is on BCM disaster recovery following major incidents, e.g., earthquakes. The standard covers prevention of disruptions and recovery from any disruptive incident.
2. In the main, the BCPG audit looked at the BCM and the areas covering emergency management and IT failures.
3. The scope of BCPG certification was not clearly defined as Stage 1 at initiation but appeared to miss key elements at Stage 2.
4. Consideration was not given to the role of BCPG support service partners in supplying incident site teams at incident指挥 when considering the call centre. Also, the assumption was made that the BCPG Tokyo office is destroyed to avoid the major customer and supplier premises. This is more likely to be the case in non-BCM critical situations.
5. BCPG staff awareness was only tested around the existence of the policy document and what actions would be taken in the case of an earthquake or blackout. BCM awareness was not tested at the auditors' location.
6. I have no confidence that BCPG for BCPG were comprehensive and covered the reality of the call centre operations or Design Services. The auditors did not verify this.
7. The importance of exercising was not fully appreciated by BCPG and there appeared to be no lessons learned in material or reports as a result of incidents already carried out. The auditors did not pursue the important areas.
8. BCPG internal audit of BCM was not effective at the time of audit, lack of training.
9. Concerns raised by the auditors (both lead and technical) did not focus down on BCM issues within BCPG. There were issues obtained in the development of the BCM and IT actions by the lead auditor.
10. Auditors were expressing opinion and giving advice to BCPG in the areas where they were experienced, management systems and IT.
11. There is a major concern about the current lack of BCM training across all areas of responsibility within BCPG. Planned courses however are of an appropriate standard and will be cascaded from auditors to other areas of responsibility.
12. The sales documentation and procedure manuals were satisfactory.
13. Individual contracts, job descriptions, and career histories were in place for all employees involved.
14. Contracts, confidentiality agreements, and codes of conduct were in place for external contractors.
Possible Outcomes

Certification/ Registration is awarded!
- surveillance audit scheduled

Provisional Certification/ Registration is awarded!
- One (or more) **minor** non-conformance areas
- Requires a program of *Preventative* and *Corrective* actions
- Time-sensitive re-examination
- May require a re-audit (more expensive)

Failed Audit
- **One** or more **major** non-conformance areas
- Multiple (?) minor non-conforming areas
Self Assessments

The Goal: SDoC

Choices

Sample Evidence
<table>
<thead>
<tr>
<th>Reference Clause</th>
<th>Element</th>
<th>Standard Area of Practice</th>
<th>Self Assessment Content</th>
<th>Self Assessment Findings</th>
<th>Note and Observations on Additional Evidence</th>
</tr>
</thead>
</table>
| 4.1.1             | Implementing and Operating the BCMS | BIA | “There shall be a defined, documented and appropriate method for determining the impact of any disruption of the activities that support the organization’s key products and services (see 3.2.1).” | Conforms | ✓ Can you produce proof that BIA interviews were conducted?  
   ✓ Do you have records showing that BIA workshops were held?  
   ☐ Do you have records showing when and how BIA surveys were used?  
   ✓ Do you have worksheets showing who conducted the BIA?  
   ☐ Does your BIA include RTO and MTTPD calculations?  
   ☐ Can you provide evidence that shows interdependencies in the BIA? |
| 4.1.2             | Implementing and Operating the BCMS | Risk Assessment Description. | | Major NonCom | ✓ Can you produce proof that BIA interviews were conducted?  
   ✓ Do you have records showing that BIA workshops were held?  
   ☐ Do you have records showing when and how BIA surveys were used?  
   ✓ Do you have worksheets showing who conducted the BIA?  
   ☐ Does your BIA include RTO and MTTPD calculations?  
   ☐ Can you provide evidence that shows interdependencies in the BIA? |
| 4.1.3             | Implementing and Operating | BIA | (Clause 4.1.3) Description. | ✗ IA or Out of Scope |  
   ☐ Can you produce proof that BIA interviews were conducted?  
   ☐ Do you have records showing that BIA workshops were held?  
   ☐ Do you have records showing when and how BIA surveys were used? |
On-going Process