ISO 22301, ISO 27031  (BS 25999-1 and BS 25999-2)
Business Continuity Management & Planning
IT Governance
CEN 667
Project proposal

• Goal of the projects are to find applicable measurement and metric methods to improve processes:
  – For 27000 series of standards 27001 and 27004 –
  – For ITIL
  – For Business Continuity and BS 25999
  – For Disaster Recovery –
  – For Penetration testing –
  – For Operational and Security Incident management
  – For Risk Management
  – Secure method for visual authentication –
  – Mobile security access with speech recognition –
  – Other agreed with lecturer

• Literature review on selected topic - between 500 and 1000 words

• Proposal / for improvements of chosen method, approach, technique, - up to 2000 words

• List of references

• Document prepared in two columns as it should

Be prepared for the conference paper

• Week report on updates

New Forensic Method for Measuring Dynamic Changes of EMF Level Limits Using Smart Dust

Author

Abstract – Devices and appliances such as transformers, mobile phones and GSM antennas, or devices motors, printers, electromagnetic fields (EMF) around them during their operation. According to an International Commission on Non-Ionizing Radiation Protection (ICNIRP) levels above 300 milligauss (mg) or 200 microtesla (aT) for occupant in general premises are considered as dangerous for human health. While this is international standard, national standards have different acceptable value levels of EMF strength around devices and antennas. Scientists from 1979 are still trying to prove connection between serious health risk and EMF. As a step to make many clear this area of research in this paper is presented new application model for monitoring dynamic changes of EMF strength levels. This because more important after European Council and World Health Organization (WHO) in the May of 2011 changed their policies referred to EMF and health risk. In this paper the health risk of EMF is not proven, and that was not an intention. Our concern are EMF strength levels around devices and appliances and more specifically GSM antennas, and how strength levels can be measured and controlled dynamically because of new knowledge by which EMF is connected to health risk. This paper presents new application model for collecting data about EMF strength levels around devices and antennas which reduce EMF in dynamic manner using

[Image of GSM antenna installed on hotel premises]
<table>
<thead>
<tr>
<th>Candidate</th>
<th>Topic</th>
<th>Literature review draft</th>
<th>Paper</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azizah Ibrahim</td>
<td>Mobile IPv6 handover packet loss avoidance</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>Emina Aaličković</td>
<td>NO</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>Jasmin Kevrić</td>
<td>Algorithm improvement for the network anomaly detection using improved KDD 2009</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adnan Miljković</td>
<td>Implementation of two factor authentication for web application</td>
<td>YES (463 words)</td>
<td></td>
</tr>
<tr>
<td>Fatih Ozturk</td>
<td>NO</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>Tarik Kraljić</td>
<td>NO</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>Adnan Kraljić</td>
<td>NO</td>
<td>NO</td>
<td></td>
</tr>
</tbody>
</table>
Business Continuity and BS 25999-1 and BS 25999-2
Business Continuity Management & Planning

IT Governance
CEN 667
<table>
<thead>
<tr>
<th>Week</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week 1</td>
<td>Introduction to IT governance</td>
</tr>
<tr>
<td>Week 2</td>
<td>Overview of Information Security standards - ISO 27000 series of standards (27001, 27002, 27003, 27004, 27005)</td>
</tr>
<tr>
<td>Week 3</td>
<td>Information Technology Service management ISO 20000-1 and ISO 20000-2</td>
</tr>
<tr>
<td>Week 4</td>
<td>ITIL</td>
</tr>
<tr>
<td><strong>Week 5</strong></td>
<td><strong>Business Continuity and Standards</strong></td>
</tr>
<tr>
<td>Week 6</td>
<td>Disaster Recovery</td>
</tr>
<tr>
<td>Week 7</td>
<td>COBIT</td>
</tr>
<tr>
<td>Week 8</td>
<td>Project implementation (ISO 10006 and ISO 27003)</td>
</tr>
<tr>
<td>Week 9</td>
<td>Midterm</td>
</tr>
<tr>
<td>Week 10</td>
<td>Risk Management (ISO 27005)</td>
</tr>
<tr>
<td>Week 11</td>
<td>Application and Network Security and security testing</td>
</tr>
<tr>
<td>Week 12</td>
<td>Specific Requirements and Controls Implementation (ISO 27002)</td>
</tr>
<tr>
<td>Week 13</td>
<td>Operational and Security Incident management</td>
</tr>
<tr>
<td>Week 14</td>
<td>Performance Measurement and Metrics (ISO 27004)</td>
</tr>
<tr>
<td>Week 15</td>
<td>Audit (ISO 19011) and Plan- Do-Check-Act improvement cycle</td>
</tr>
</tbody>
</table>
Business Continuity Planning Methodology

BC Planning Begins
- Create a Business Continuity Policy
- Establish a BCP Steering Committee
- Establish a BC Plan Development Project

BCP Management
- Coordinate BCP with Pertinent Laws, Regulations, and Industry Standards
- Coordinate with Other Internal/External BCP/Related Agencies
- Plan Development Project
- Risk Management
- Business Impact Analysis
- BC Strategy Development
- BC Plan Development

Time
- Complete BC Plan
- Business Disruption
- Maintain Disaster Readiness
- Execute BC Plan

Dr. Akhtar Syed, Ph.D., CISSP, CBRP
Afsar Syed, BMath., ABCP, CBRP
Objectives

• Approch for Building & Embedding a Business Continuity management culture
• Understanding legal & policy requirements
• Overview of the Business Continuity Management (BCM) process model
• Creating the Business Continuity Plan (BCP)
• Overview of the BCM life cycle
• Introduction to Risk Management Guide & Questionnaire
• BS 25999-1 Business continuity management – Part 1, Code of Practice
• BS 25999-2 Business continuity management – Part 2, Specification

References: BCI Institute, DRI International

14 Business continuity management

14.1 Information security aspects of business continuity management

14.1.1 Including information security in the business continuity management process
14.1.2 Business continuity and risk assessment
14.1.3 Developing and implementing continuity plans including information security
14.1.4 Business continuity planning framework
14.1.5 Testing, maintaining and re-assessing business continuity plans

British standards for BC

BS 25999-1 Business continuity management – Part 1, Code of Practice
BS 25999-2 Business continuity management – Part 2, Specification
Study cases revealed
Buncefield fuel depot (Hemel Hempstead) London, December 2005

1. Map showing the location of Buncefield fuel depot near London.
2. Satellite image of the Buncefield fuel depot.
3. Smoke cloud over the area on 9th December 2005.
4. View from a high vantage point of the depot.
5. Close-up of the smoke plume.
Emergency Response Team / Center for Port Authority

Responsible for 3 airports, tunnels, bridges, buses and trains meet at Marriott Hotel.
Suicide attack on Manhattan
Two aircraft hijacked from Boston smash into The World Trade Center, causing collapse of the structures and massive casualties.

9:03 a.m.
United Airlines Flight 175 crashes into South Tower

10:05 a.m.
South Tower 2 collapses

8:45 a.m.
American Airlines Flight 11 crashes into North Tower

5:25 p.m.
Tower 7 collapses

10:28 a.m.
North Tower 1 collapses

Hudson River

World Trade Center

World Financial Center

NEW YORK

NEW JERSEY

Brooklyn Bridge

1 MILE
Major data loss causes

- Hardware or System Malfunctions 44%
- Human Error 32%
- Software Corruption 14%
- Computer Viruses 7%
- Natural Disasters 3%

Source Gartner
Business Continuity Management

The advance planning and preparations which are necessary to identify the impact of potential technology losses, develop and test recovery plan(s) which ensure continuity of business services in the event of an emergency or disaster, and administer a comprehensive training, testing, and maintenance program.
Other BC definition

What is Busines Continuity Plan? (BS 25999-1 and -2) and ISO 27001:2005 in section 14.

Business Continuity Plan (BCP) represents overall plan of activities necessary to preserve operations / functions of company in case that activities are disrupted by any kind of incident or disaster.
Business Continuity Management

Process Steps

Post planning

Pre-planning

Maintain & Update

Project Initiation

Functional Requirements

Design & Develop

Implementation

Testing & Executing

Planning

Used by permission of DRI International
- Problem definition
- Policy statement
- Project sponsor
Problem Definition

Disaster Recovery vs. Business Continuity

– Late 1960s  First DR plan – IT only – US
– 1970s       IT - Dependence on centralized processing
               I/S batch mode (not interactive), mainly DR
– 1980s       Online – Interactive processing emerges
               Specialized software started appearing
– 1990s       Recover the business, not just IS
               Online real time processing
               Increased number of disasters
– 2000s       Reduced recovery time objectives
               Increased number of disasters
               Character and integrity of organizations are more in question
Problem Definition

Technology Implications

– Business units have fewer resources, increased liabilities, technology upgrades and training demands

– Business leaders are faced with mandatory planning, scrutiny and accountability, implementation must be affordable, and consider strategic vs. fiscal

– IT recovery managers have shorter recovery time objectives, lower cost solutions to meet business requirements
Policy Statement

• Builds and embeds a business continuity management culture. This is where it becomes an integral part of the organization’s strategic day to day management.

• Addresses:
  – program scope
  – goals
  – roles & responsibilities
  – reporting
  – testing
Industry best practices: senior management sponsorship is essential to successfully drive the BCM project by publicizing a clearly defined BCM policy and appointment of a BCM champion to implement the policy across all operational units.
• Understanding Business needs
• Business Impact Analysis (BIA)
• Risk Assessment (RA)
Understanding Business

• Analysis of the operational aspects of an organization which BCM is based on to establish what is critical for its continuance

• Analysis should consider the following:
  – What are your key business objectives
  – What are the deliverables of the business service
  – When are the business objectives to be achieved
  – Who is involved (both internally and externally)
  – How are they to be achieved
Mission Critical Activities (MCA)

Time sensitive critical business activities & processes required for normal daily delivery of goods and services
MCAs

• Determining MCAs include two complimentary processes
  – Business Impact Analysis (BIA)
  – Risk Assessment (RA)
BIA

Establish critical MCA’s, their recovery priorities and interdependencies so that recovery time objectives and recovery point objectives can be set
BIA

Purpose

• Supports the whole BCM process
• Linear process used to identify, quantify & qualify impacts on an organization of a loss, interruption or disruption of a (MCA) & its dependencies
• Identifies the minimum level of resources required to achieve its RTO and RPO for MCA
• BIA establishes the organizations risk appetite
• Conducted every 12 months
BCM Lifecycle

Start → BIA → MCA → RA → BCP → Testing & Exercising → Maintenance & Update → Continuous Analysis

"Focus"

Incorporate as part of your daily business strategy

Organizational Placement
Vision & Policy Statement

Project Initiation
Run Time Obj
Recovery Point Obj

Identify
Analyze
Manage

Reduction
Response
Recovery & Restart
Execution

Change Management

Fundamental Requirements

Full Continuity

Cost Analysis to close gaps

Design & Development Implementation

Incorporate as part of your daily business strategy
Risk

The potential exposure of a mission critical activity to damage
Risk Management Guide

Present an approach for risk management to assist state agencies in assessing risk that could impair their ability to deliver critical services to state citizens
Scope

Approach explains how to assess the risk that is associated with a particular line of business (MCA) that relies on IT systems
Assumptions

• The line of business has been identified
• The line of business relies on identified automated system(s)
• The automated system has been identified as critical to support the line of business
• The business owner(s) have been identified
• Staff has been identified to facilitate the risk assessment process
• The line of business is exposed to risks other than IT
• Legal parameters that control delivery of program services are understood
Risk Types

• **Business Risk** – The cost and/or lost revenue or funding associated with an interruption to normal business operations.

• **Organizational Risk** – The direct or indirect loss resulting from one or more of the following:
  – Inadequate or failed internal processes
  – People
  – Systems
  – External events

• **Information Technology Risk** – The loss of an automated system, network or other critical information technology resource that would adversely affect business processes.
Risk Impact Categories

• **Operations** – Functions that support delivery of agency business services (facilities and space allocation, personnel, purchasing, financial, communications, etc.)

• **Technology** – Information assets that support the IT Infrastructure (security, hardware, software, middleware, network and communication systems, etc.)

• **Legal** – Parameters established by legislative mandates, federal and state regulations, policy directives and executive orders that impact delivery of program services.

• **Citizen Services** – Program services mandated by charter, legislation, or policy that provides for the delivery of the state’s business (education, human services, highways, law enforcement, health and safety, unemployment benefits, vital records, etc.)

• **Reputation** – General estimation, by the public, on how state services are delivered (integrity, credibility, trust, customer satisfaction, image, media relations, political involvement.)
Rating Scale

• **Low** – If an event could be expected to have a limited adverse effect on agency operations (including mission, functions, image or reputation, agency assets, or individuals; and cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.

• **Moderate** – If an event could be expected to have a serious adverse effect on agency operations, agency assets or individuals, and cause significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.

• **High** – If an event could be expected to have a severe or catastrophic adverse effect on agency operations, agency assets, or individuals; and cause a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.
Risk Assessment Approach

Phase I – Identify risks
Phase II – Analyze risks
Phase III – Manage risks
Phase I

Identify the Risks

– Business leaders / Owners complete
– Determine areas of risk that result in additional analysis in Phase II
Phase II

Risk Analysis

– Evaluate results identified in phase I
– Service delivery owners complete
– Determine significance of risk
– Utilize reference sources to complete analysis such as facilities, people, inter-dependencies, equipment / software inventories
– Determine risks that require a gap analysis
Phase III

Manage risks

– Business leaders / service delivery owners complete
– Review risk management control strategies
– Where the risk level remains unacceptable, design new controls or consider other options
– Provide a cost benefit analysis for business sponsor based on defined risk appetite
– Consider risk strategies such as:
  • Transfer the risk
  • Accept the risk
  • Reduce the risk
  • Avoid the risk
– Obtain management review & signoff of risk analysis
- Definition
- Consideration
- Plan elements
- Plan framework structure
Business Continuity Planning (BCP)

The process of developing advance arrangements and procedures that enable an agency to respond to an event in such a manner that mission critical activities supported by information technology (IT) continue with planned levels of interruption or essential change.
BCP Considerations

• Structure must be tailored to the needs and requirements of the organization
• Flexible to allow addition, modification & maintenance
• Minimize dependencies on individuals or outside entities
• Complete, current & tested
• Includes a clearly defined & documented change management process
BCP Considerations

• Includes a method to establish a clearly defined & documented BCP that is agreed to & signed off by the accountable business owners of the MCA and their dependencies

• Includes resource recovery solutions that are prioritized & tiered dependent upon their criticality to the organization as defined by the BIA
BCP Considerations

• BCM solutions supported by a contractual agreement should include option for renewal, conditions that enable the verification of the agreed level of service (upsizing or downsizing)

• A full continuity plan that includes
  – Reduction
  – Response
  – Recovery & resumption
  – Restoration & return
BCP Plan Elements

• Systems Overview
• Dependencies (business partners, vendors)
• Critical staff & emergency contact information
• Critical equipment & asset inventory (hardware, etc.)
• Critical application inventory & data backups
• Plan activation & notification procedures, call trees
• Alternate work sites identified, off-site storage
• Staff succession plan, business recovery teams
• Security requirements
• Recovery strategies, work around procedures, resumption
• Test schedule
• Procedures for plan distribution & executive signoff
• Emergency Response (evacuation)
• Delegation / designation of authority
• Command, control & management operations center
• Vendor contracts
• Escalation, notification, plan activities
• Training & awareness programs
• Scenario to execute the plan
  – Declare disaster
  – Execute recovery operations
• Definition
• Why testing is important
• Types of tests
• Establishing a testing plan
Testing

Generic phrase used to describe the critical BCM process of exercising strategies & BCP plans, rehearsing team members & staff, testing of systems (technology infrastructure & administrative) to demonstrate a BCM competence and capability.
Why Testing Is Important

• Evaluate & enable the continuous improvement of the organization’s BCM capability to recover mission critical activities, and their dependencies within the designated timeframe

• Evaluate & enable the continuous improvement of the organization’s crisis management plan execution
# Test Methodologies

<table>
<thead>
<tr>
<th>Type</th>
<th>Techniques</th>
<th>Process</th>
<th>Participants</th>
<th>Frequency</th>
<th>Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desk Check</td>
<td>• Audit</td>
<td>Review and Challenge the contents of the plan.</td>
<td>• Author of plan</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>• Validation</td>
<td></td>
<td>• Independent checkers</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Verification</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Walkthrough</td>
<td>• Scenario</td>
<td>Extended Desk Check to check interaction and the roles of participants</td>
<td>• Author of plan</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Plan and/or Infrastructure</td>
<td>• Freeplay</td>
<td></td>
<td>• Main participants</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simulation</td>
<td>• Controlled</td>
<td>Incorporates associated plans:</td>
<td>• Main Participants</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>• Timelapse</td>
<td>• Business</td>
<td>• Participants</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unannounced</td>
<td>• Site/Buildings</td>
<td>• Facilitator</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Live</td>
<td>• Communication</td>
<td>• Observers</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Tabletop</td>
<td>• Public Relations</td>
<td>• Co-ordinators</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Individual Component(s)</td>
<td>• ITRD</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Functions</td>
<td>• Integrated Components</td>
<td>• BCM</td>
<td>• Resource Recovery Suppliers</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Full Plan</td>
<td></td>
<td>• Resource Recovery</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Suppliers</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(Adapted from Source: Elliot, Swartz and Herbane 1999 p.84)
Test Plan

• Begin simple, escalate gradually
• Resources planned for availability during an actual event should participate during the test
• Adoption of a structure & systematic approach to promote a greater understanding of the process
• Obtain the professional commitment and active participation of managers where success is dependent
• Ensure testing is performed on a defined timeline where lessons learned can be incorporated into BCM
• Ensure test plan remains current and viable in line with organizational change & current risk practice
• A BCM maintenance process that requires interaction with a wide range of managerial & operational roles from a business & technical perspective
• A process that maintains the whole of the organization’s BCM capability
• Identifies & includes changes to organization’s processes & systems and validates effective change control procedures
• Date of last & next review is clearly identified & documented together with the role to complete the task
BCM Lifecycle

"Focus"

Start → BIA → MCA → RA → BCP → Testing & Exercising → Maintenance & Update → Continuous Analysis

Project Initiation → Run Time Obj → Recovery Point Obj → Identify Analyze Manage → Reduction Response → Recovery & Restart Execution → Recurring Process

Organizational Placement Vision & Policy Statement → Cost Analysis to close gaps → Design & Development Implementation

Incorporate as part of your daily business strategy

Fundamental Requirements → Full Continuity → Change Management
Questions & Answers
Thank You!