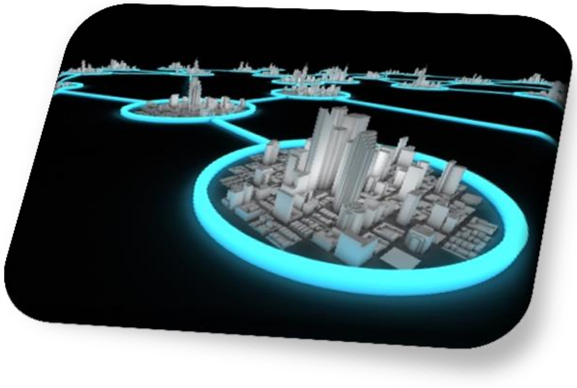
AUDIT BUSINESS CONTINUITY FOR CRITICAL INFRASTRUCTURES (AUDBCXCI)

“Manage today, secure tomorrow!”

Andino, Á.

European M.Sc. in Project Management
M.Sc. in Information Security
B.Sc. in Computer Science

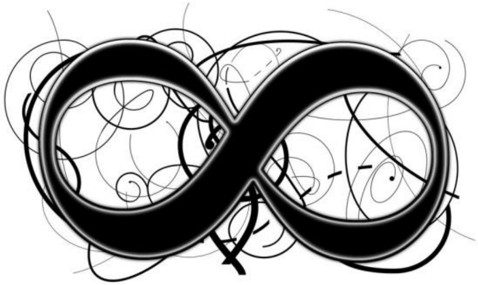
Index



1. Introduction
2. MSc InfoSec MT
3. EU-MSc PM MT
4. Research
5. Questions
6. References

Index

1. ***Introduction***
    1. **InfoSec**
    2. **Audit**
    3. **Business Continuity**
2. MSc Infosec MT
3. EU-MSc PM MT
4. Research

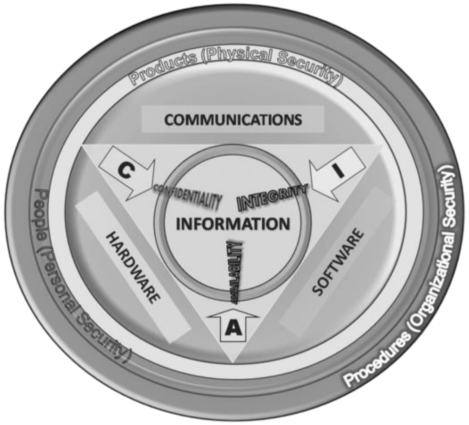


1. Introduction

1.1. Information Security (InfoSec)

- **Assets:**

- **InfoSec**: "Information Security ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity), and non-access when required (availability)" (ISACA)
- InfoSec **core principles** (CIA Triad)
  - **Confidentiality**
  - **Integrity**
  - **Availability**
  - ***Authenticity***
  - ***Non-repudiation***


Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
AVAILABILITY
HARDWARE
SOFTWARE
A
People (Personal Security)
Procedures (Organizational Security)

https://www.isaca.org/Pages/default.aspx
http://www.pmi.org/
http://dictionary.cambridge.org/dictionary/british/security_1?q=security

1. Introduction

1.2. Audit (AUD) (1/4)

“Absolute security does/may not exist.”

- **Risk**: “An uncertain event or condition that, if it occurs, has a positive or negative effect on one or more project objectives” (PMI)

Risk = [Likelihood of occurrence] x [Impact of the incident]

- **AUD**: “Systematic, independent and documented process for obtaining audit evidence and evaluating IT objectively to determine the extent to which the audit criteria are fulfilled” (ISO/DIS 22313:2012)

DIS = Draft Int. STD
Bundesamt für Sicherheit in der Informationstechnik
https://www.bsi.bund.de/DE/Home/home_node.html

1. Introduction

1.2. Audit (AUD) (1/4)

- **ISAUD Phases**

Phase	Task	Description	Time in %
1	**Preparation of the IS audit**	At the beginning of the procedure, the most important general conditions are determined and the necessary documents are requested in an opening meeting between the organisation and IS audit team.	5
2	**Creation of the IS audit plan**	Based on the documents then made available, the IS audit team gets a picture of the organisation to be examined and creates the IS audit plan.	15
3	**Revision of the documents**	Based on the IS audit plan, the contents of the available documents are assessed. If necessary, additional documents are requested. Based on the revision of the documents and the IS audit plan (which is updated during this time), the chronological and organisational terms of the on-site examination are co-ordinated together with the contact person in the organisation.	20
4	**On-site examination**	The on-site examination starts with an opening meeting with the main participants. After that, interviews are conducted, the site is inspected, and a preliminary evaluation is performed. The on-site examination terminates with a closing meeting.	**35**
5	**Evaluation of the on-site examination**	The information obtained during the on-site examination is consolidated further and evaluated by the IS audit team.	5
6	**Creation of the IS audit report**	The results of the IS audit are summarised in an IS audit report at the end of the review. This report is provided to the organisation audited.	20

DIS = Draft Int. STD
Bundesamt für Sicherheit in der Informationstechnik
https://www.bsi.bund.de/DE/Home/home_node.html

1. Introduction

1.2. AUD: Processes (3/5)

Audit Processes	
Nr.	Process
0	Define Audit Subject and Objective
1	Defining Audit Scope
2	Gather Information
3	Audit Planning
4	Risk Management Analysis
5	Gap Analysis
6	BCP & DRP Process Review
7	Mitigating Report
8	ISMS Specification & Detailing
9	Information Capturing
10	SOA Review
11	Communication to IT CIO/Management/Director
12	Audit Report
13	Follow-up Activities
14	Document Lessons Learned

1. Introduction

1.2. AUD (4/5)

- **ISAUD Team**: 2-3 auditors
- **ISAUD Professional Ethics** (ISACA)
  1. **Support implementation** and **encourage compliance**
  2. **Objectivity**
  3. **Serve in the interest** of stakeholders **lawfuly** and **honestly** (Independence)
  4. **Privacy and confidentiality**
  5. **Professional competence**
  6. **Inform** of results
  7. **Support the professional education of stakeholders**
- **ISAUD Types**
  - *Area*: Financial/Forensic/DF/ISMS/BC/…
  - *Auditor*: Internal/External
  - *Cycled/Individual*: IS cross-cutting AUD/IS partial AUD (BSI)
    - IS cross-cutting AUD → Federal Agency AUD at least every 3 years
    - IS partial AUD → limited to a section of the ORG
  - InfoSec objective:
    - Certification
    - Risk Management
    - Digital Forensics

1. Introduction

1.2. AUD: Tech & Doc (5/5)

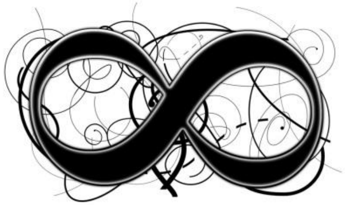
- **ISAUD Techniques** (BSI)
  - **Verbal questioning**
  - **Visual inspection**
  - **Observations**
  - **Analysis of files**
  - **Technical examination**
  - **Database analysis**
  - **Written questions**

- **ISAUD Documents** (ISACA)
  - **Planning** and preparation of the audit **scope** and **objectives**
  - **Description and/or walkthroughs**
  - **Audit program**
  - **Audit steps** performed and **audit evidence** gathered
  - Use of **services of other auditors and experts**
  - Audit **findings, conclusions, and recommendations**
  - Audit **documentation relation with document identification and dates**
  - **AUD Report**

1. Introduction

1.3. Business Continuity (BC) & BC Management (BCM)

- **BC**
  - Strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level.
- **BCM**
  - Holistic management process that identifies potential threats to an organization and the impacts to business operations of those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

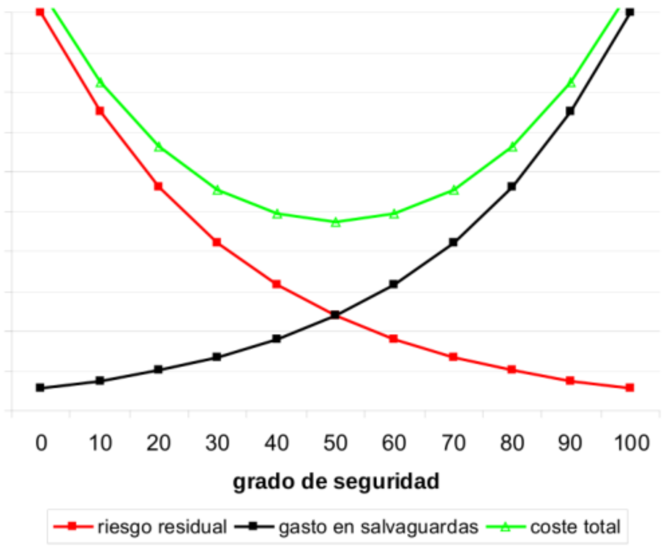


ISO 22313:2012 -- Societal security -- Business continuity management systems -- Guidance

1. Introduction

1.3. BC: Advantages vs. Disadvantages

Criteria	BC Advantages	BC Disadvantages
Time	Long-term experience in the application of BCM in an organization. **Assurance of rapid recovery** of normal operating functions	**Time-consuming** requirement to implement BCM in the organization
Finance	Competitive advantage given by **response to crisis** situations and **preservation of critical knowledge** in the organization	**Bad implementation** of BCM leads to **financial losses** in the organization
Structure	**Specific BCM for each organization** in each sector	**Uneven utilization** of BCM across **individual economic sectors.** The maximum utilization is the banking sector
Human Resources	**Retention of critical knowledge** and key employees in the organization	**Specialists leaving to join the competition**. Poor communications
Quality	Q’ assurance	Standardized Q’
Safety & Security	Ensures safety & security	Does not prevent bugs

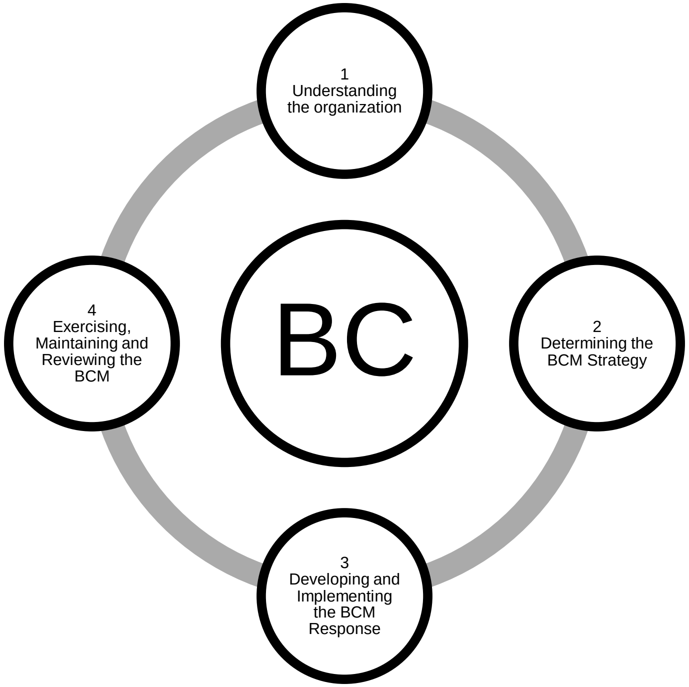


C of Countermeasures < C of Assets

N. W. Wong, “The strategic skills of business continuity managers: putting business continuity management into corporate long-term planning,” *Journal of Business Continuity & Emergency Planning*, vol. 4, no. 1, pp. 62-68, 2009.

1. Introduction

1.3. BC: Phases


1
Understanding the organization
2
Determining the BCM Strategy
3
Developing and Implementing the BCM Response
4
Exercising, Maintaining and Reviewing the BCM
BC

Nr.	Phase	Description
1	**Understanding the Organization**	Obtain comprehensive knowledge (transparency) of your own organisation (e.g. by performing a BIA and a RA)
2	**Determining BC Strategy**	Development of BC Strategy options
3	**Developing and Implementing the BCM Response**	Development and implementation of reaction measures and BCP
4	**Exercising, Maintaining and Reviewing the BCM**	Performing BCM exercises and examining and refining the BCP and BCM safeguards

BS 25999-2:2007 Specification for Business Continuity Management

1. Introduction

1.3. BC: Documents

- **Risk Assessment (RA):** determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat
- **Business Impact Analysis (BIA)**: evaluate the critical processes (and IT components supporting them) and to determine time frames, priorities, resources and interdependencies
- **BC Strategy**: based on BIA and risk assessment → **BCM Policy**: policies should be brief and concise but informative
- **Business Continuity Plan (BCP)**: or "Business Continuity and Resiliency Planning (BCRP)", based on BIA, is a roadmap to continue operations in adversity
- **Disaster Recovery Plan (DRP)**: included in BCP or separate Doc. Manages availability and restore critical processes/IT services in the event of interruption

https://www.isaca.org/Pages/default.aspx

1. Introduction

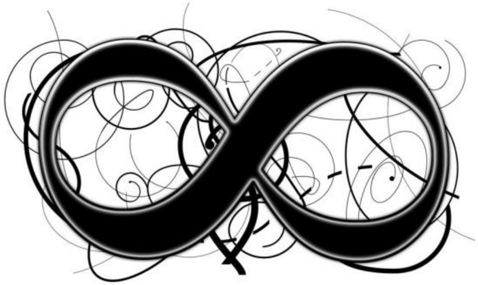
1.3. BC: Critical Infrastructures

- **Critical Infrastructure (CI)**: systems whose incapacity or destruction would have a debilitating effect on the safety, security and economic sustainability of an enterprise, community or nation
- **14 Areas of CI**
  - Agriculture & Food
  - Water
  - Public Health
  - Emergency Services
  - Government
  - Defence Industrial Base
  - Information and Telecommunications,
  - Banking and Finance
  - Energy
  - Transportation
  - Chemical Industry and Hazardous Materials
  - Postal and Shipping
  - National monuments and icons
  - Critical Manufacturing
- **CI Vulnerabilities Groups**
  - Data
  - Security administration
  - Architecture
  - Network/Communications
  - Platforms to assist in determining optimal mitigation strategies
- **CI Threats Categories**
  - Natural
  - Human-caused
  - Accidental or Technical
- **CI Attacks Effects**
  - Direct effects
  - Indirect Effects

https://www.isaca.org/

Index

1. Introduction
2. ***MSc InfoSec MT***
    1. **What?**
    2. **How?**
    3. **Results**
3. EU-MSc PM MT
4. Research



2. MSc InfoSec MT

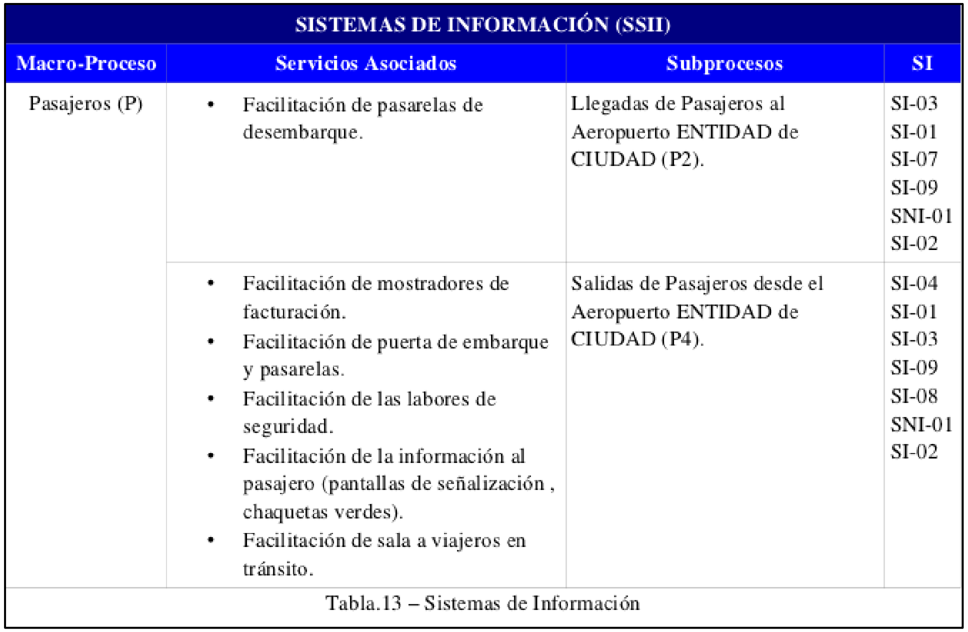
2.1. What?

- Title: *“Audit adequacy to Standards and compliance of Risk Assessment and subsequent Business Continuity Plan”*
    - Scope
    - Legal & Regulatory Framework
    - Scenarios
    - Risk Assessment (RA)
    - Risk Management (RM)
    - Business Impact Analysis (BIA)
    - Business Continuity Plan (BCP)

2. MSc InfoSec MT

2.2. How?

- Scenario
  - Macro-Processes
    - “P” → P2, P4
    - “L” → L2, L4
    - “A” → A2, A4
  - Assets
  - Resources



SISTEMAS DE INFORMACIÓN (SSII)

Macro-Proceso	Servicios Asociados	Subprocesos	SI
Pasajeros (P)	• Facilitación de pasarelas de desembarque.	Llegadas de Pasajeros al Aeropuerto ENTIDAD de CIUDAD (P2).	SI-03 SI-01 SI-07 SI-09 SNI-01 SI-02
	• Facilitación de mostradores de facturación. • Facilitación de puerta de embarque y pasarelas. • Facilitación de las labores de seguridad. • Facilitación de la información al pasajero (pantallas de señalización , chaquetas verdes). • Facilitación de sala a viajeros en tránsito.	Salidas de Pasajeros desde el Aeropuerto ENTIDAD de CIUDAD (P4).	SI-04 SI-01 SI-03 SI-09 SI-08 SNI-01 SI-02

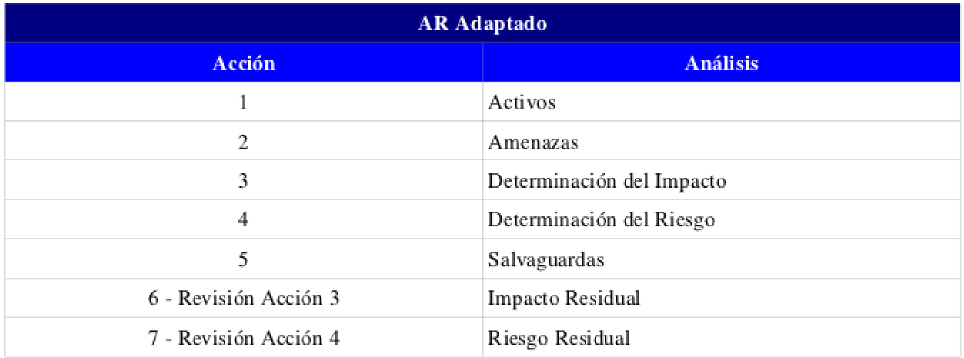
Tabla.13 – Sistemas de Información

- Legal & Regulatory Framework:
  - EU Privacy Law
  - LOPD (ES Privacy Law)
  - Passenger rights
  - BOE (ES official)
  - Environmental Law
  - IS Law

  - ISO/IEC 13335:2004
  - ISO/IEC 15408:2005
  - ISO/IEC 27001:2005
  - ISO/IEC 27002:2005
  - BSi 25999-1:2006 (ISO 22313)
  - BSi 25999-2:2007 (ISO 22301)

2. MSc InfoSec MT

2.3. Results: Risk Assessment (RA)



AR Adaptado	
Acción	**Análisis**
1	Activos
2	Amenazas
3	Determinación del Impacto
4	Determinación del Riesgo
5	Salvaguardas
6 - Revisión Acción 3	Impacto Residual
7 - Revisión Acción 4	Riesgo Residual

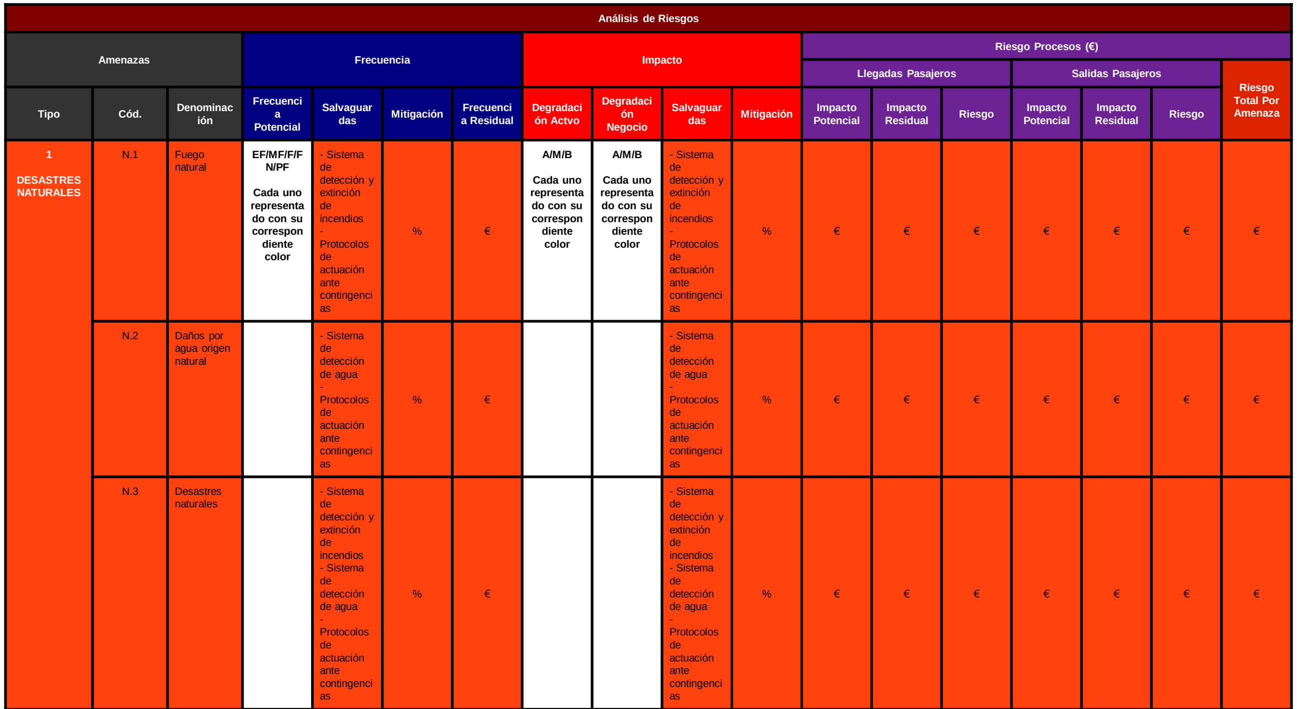
Tabla.25 – AR Adaptado

Risk assessment:

1. Assets
2. Threats
3. Impact
4. Risk
5. Countermeasures
6. Residual Impact
7. Residual Risk

Risk assessment:

1. Threats
2. Frecuency
3. Impact
4. Risk

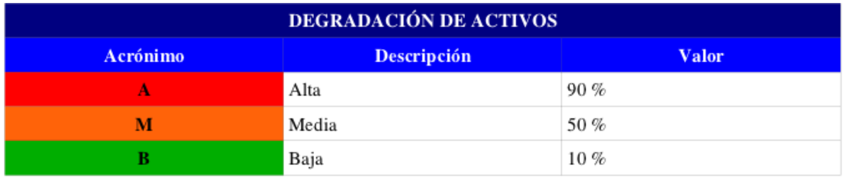


Análisis de Riesgos																	
Amenazas			Frecuencia				Impacto				Riesgo Procesos (€)						
											Llegadas Pasajeros			Salidas Pasajeros			Riesgo Total Por Amenaza
Tipo	Cód.	Denominación	Frecuencia Potencial	Salvaguardas	Mitigación	Frecuencia Residual	Degradación Actvo	Degradación Negocio	Salvaguardas	Mitigación	Impacto Potencial	Impacto Residual	Riesgo	Impacto Potencial	Impacto Residual	Riesgo	
1 DESASTRES NATURALES	N.1	Fuego natural	EF/MF/F/FN/PF Cada uno representado con su correspondiente color	- Sistema de detección y extinción de incendios - Protocolos de actuación ante contingencias	%	€	A/M/B Cada uno representado con su correspondiente color	A/M/B Cada uno representado con su correspondiente color	- Sistema de detección y extinción de incendios - Protocolos de actuación ante contingencias	%	€	€	€	€	€	€	€
	N.2	Daños por agua origen natural		- Sistema de detección de agua - Protocolos de actuación ante contingencias	%	€			- Sistema de detección de agua - Protocolos de actuación ante contingencias	%	€	€	€	€	€	€	€
	N.3	Desastres naturales		- Sistema de detección y extinción de incendios - Sistema de detección de agua - Protocolos de actuación ante contingencias	%	€			- Sistema de detección y extinción de incendios - Sistema de detección de agua - Protocolos de actuación ante contingencias	%	€	€	€	€	€	€	€

2. MSc InfoSec MT

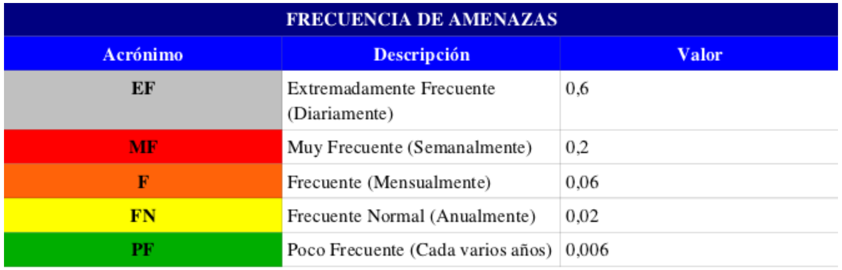
2.3. Results: Risk Management (RM)

- RM:
  1. Values interpretation
  2. Countermeasures selection
  3. Gains & Losses
  4. Direction attitude
  5. Assets review



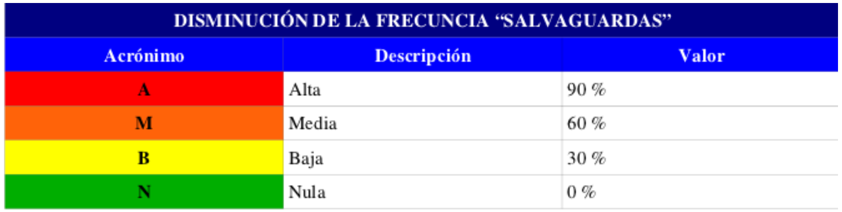
DEGRADACIÓN DE ACTIVOS		
Acrónimo	**Descripción**	**Valor**
A	Alta	90 %
M	Media	50 %
B	Baja	10 %

Tabla.28 – Criterios de Valoración de Degradación de Activos



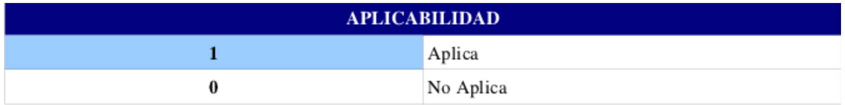
FRECUENCIA DE AMENAZAS		
Acrónimo	**Descripción**	**Valor**
EF	Extremadamente Frecuente (Diariamente)	0,6
MF	Muy Frecuente (Semanalmente)	0,2
F	Frecuente (Mensualmente)	0,06
FN	Frecuente Normal (Anualmente)	0,02
PF	Poco Frecuente (Cada varios años)	0,006

Tabla.29 – Criterios de Valoración de Frecuencia de Amenazas



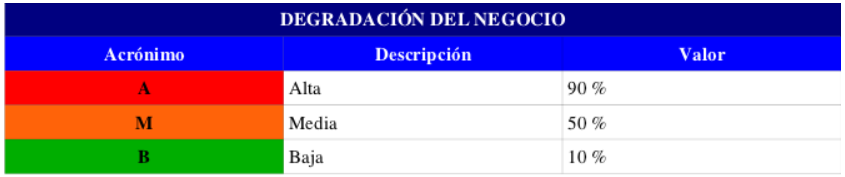
DISMINUCIÓN DE LA FRECUENCIA "SALVAGUARDAS"		
Acrónimo	**Descripción**	**Valor**
A	Alta	90 %
M	Media	60 %
B	Baja	30 %
N	Nula	0 %

Tabla.31 – Criterios de Valoración de Disminución de la Frecuencia "Salvaguardas"



APLICABILIDAD	
1	Aplica
0	No Aplica

Tabla.33 – Criterios de Valoración de Aplicabilidad

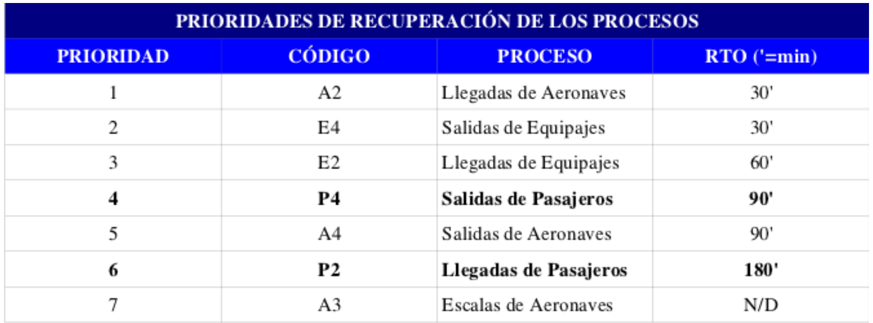


DEGRADACIÓN DEL NEGOCIO		
Acrónimo	**Descripción**	**Valor**
A	Alta	90 %
M	Media	50 %
B	Baja	10 %

Tabla.30 – Criterios de Valoración de Degradación del Negocio

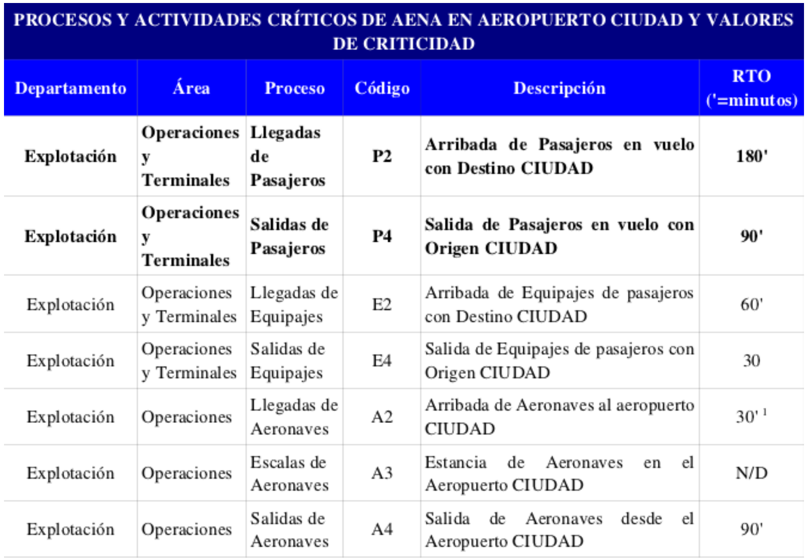
2. MSc InfoSec MT

2.3. Results: Business Impact Analysis (BIA)



PRIORIDADES DE RECUPERACIÓN DE LOS PROCESOS			
PRIORIDAD	CÓDIGO	PROCESO	RTO ('=min)
1	A2	Llegadas de Aeronaves	30'
2	E4	Salidas de Equipajes	30'
3	E2	Llegadas de Equipajes	60'
4	**P4**	**Salidas de Pasajeros**	**90'**
5	A4	Salidas de Aeronaves	90'
6	**P2**	**Llegadas de Pasajeros**	**180'**
7	A3	Escalas de Aeronaves	N/D

Tabla.68 – Prioridades de Recuperación de los Procesos



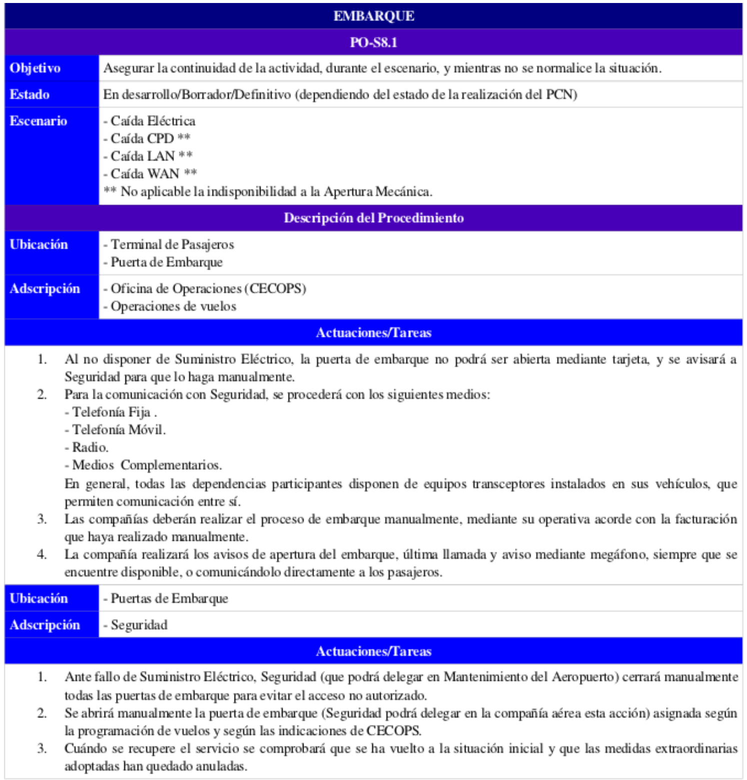
PROCESOS Y ACTIVIDADES CRÍTICOS DE AENA EN AEROPUERTO CIUDAD Y VALORES DE CRITICIDAD					
Departamento	Área	Proceso	Código	Descripción	RTO ('=minutos)
Explotación	**Operaciones y Terminales**	**Llegadas de Pasajeros**	**P2**	**Arribada de Pasajeros en vuelo con Destino CIUDAD**	**180'**
Explotación	**Operaciones y Terminales**	**Salidas de Pasajeros**	**P4**	**Salida de Pasajeros en vuelo con Origen CIUDAD**	**90'**
Explotación	Operaciones y Terminales	Llegadas de Equipajes	E2	Arribada de Equipajes de pasajeros con Destino CIUDAD	60'
Explotación	Operaciones y Terminales	Salidas de Equipajes	E4	Salida de Equipajes de pasajeros con Origen CIUDAD	30
Explotación	Operaciones	Llegadas de Aeronaves	A2	Arribada de Aeronaves al aeropuerto CIUDAD	30' [1]
Explotación	Operaciones	Escalas de Aeronaves	A3	Estancia de Aeronaves en el Aeropuerto CIUDAD	N/D
Explotación	Operaciones	Salidas de Aeronaves	A4	Salida de Aeronaves desde el Aeropuerto CIUDAD	90'

Tabla.67 – Procesos y Actividades Críticos de AENA en Aeropuerto CIUDAD y Valores de Criticidad

2. MSc InfoSec MT

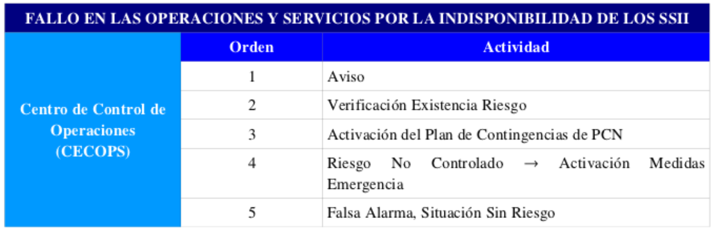
2.3. Results: Business Continuity Plan (BCP)

- BCP:
  - IS unavailability
  - P2 & P4



EMBARQUE	
PO-S8.1	
Objetivo	Asegurar la continuidad de la actividad, durante el escenario, y mientras no se normalice la situación.
Estado	En desarrollo/Borrador/Definitivo (dependiendo del estado de la realización del PCN)
Escenario	- Caída Eléctrica - Caída CPD ** - Caída LAN ** - Caída WAN ** ** No aplicable la indisponibilidad a la Apertura Mecánica.
Descripción del Procedimiento	
Ubicación	- Terminal de Pasajeros - Puerta de Embarque
Adscripción	- Oficina de Operaciones (CECOPS) - Operaciones de vuelos
Actuaciones/Tareas	
1. Al no disponer de Suministro Eléctrico, la puerta de embarque no podrá ser abierta mediante tarjeta, y se avisará a Seguridad para que lo haga manualmente. 2. Para la comunicación con Seguridad, se procederá con los siguientes medios: - Telefonía Fija . - Telefonía Móvil. - Radio. - Medios Complementarios. En general, todas las dependencias participantes disponen de equipos transceptores instalados en sus vehículos, que permiten comunicación entre sí. 3. Las compañías deberán realizar el proceso de embarque manualmente, mediante su operativa acorde con la facturación que haya realizado manualmente. 4. La compañía realizará los avisos de apertura del embarque, última llamada y aviso mediante megáfono, siempre que se encuentre disponible, o comunicándolo directamente a los pasajeros.	
Ubicación	- Puertas de Embarque
Adscripción	- Seguridad
Actuaciones/Tareas	
1. Ante fallo de Suministro Eléctrico, Seguridad (que podrá delegar en Mantenimiento del Aeropuerto) cerrará manualmente todas las puertas de embarque para evitar el acceso no autorizado. 2. Se abrirá manualmente la puerta de embarque (Seguridad podrá delegar en la compañía aérea esta acción) asignada según la programación de vuelos y según las indicaciones de CECOPS. 3. Cuándo se recupere el servicio se comprobará que se ha vuelto a la situación inicial y que las medidas extraordinarias adoptadas han quedado anuladas.	

Tabla.82 – Plan de Contingencias Proceso Pasajeros "Embarque"

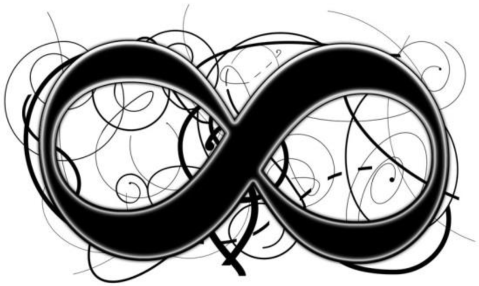


FALLO EN LAS OPERACIONES Y SERVICIOS POR LA INDISPONIBILIDAD DE LOS SSII		
Centro de Control de Operaciones (CECOPS)	Orden	Actividad
	1	Aviso
	2	Verificación Existencia Riesgo
	3	Activación del Plan de Contingencias de PCN
	4	Riesgo No Controlado → Activación Medidas Emergencia
	5	Falsa Alarma, Situación Sin Riesgo

Tabla.72 – Fallo en las Operaciones y Servicios por la Indisponibilidad de los SSII

Index

1. Introduction
2. MSc InfoSec MT
3. ***EU-MSc PM MT***
   1. **Obj.**
   2. **How?**
   3. **What?**
   4. **Results**
   5. **Conclusion**
4. Research



3. EU-MSc In PM MT

3.1. Objective

- Title: *“Business Continuity, Audit and Information Security: Frameworks, Standards, and New Solutions”*

1. Overview of actual InfoSec frameworks and standards with emphasis on audit processes within those.
2. IT frameworks and standards analysis: Advantages & Disadvantages.
3. Auditing BC and InfoSec processes optimization and new solutions proposal.

3. EU-MSc PM MT

3.2. How?

- BC, AUD, InfoSec related FW & STD comparison
- **Relevant FW**
  - ***PMBOK***: Project Management Book Of Knowledge;
  - ***COBIT***: Control Objectives for Information and Related Technology is a framework created by ISACA for IT management and IT governance;
  - ***ITIL***: Information Technology Infrastructure Library is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business.
- **Relevant STD**
  - ***ISM Standards***:
    - ISO/IEC 20000 – International Standard for IT Service Management
    - ISO 31000 – family of standards relating to RM
      - ISO 31000:2009 - Principles and Guidelines on Implementation
      - ISO/IEC 31010:2009 - Risk Management - Risk Assessment Techniques
      - ISO Guide 73:2009 - Risk Management - Vocabulary
    - ISO/IEC 27001:2005 – (formerly BS 7799-2:2002, and last update ISO/IEC 27001:2013) Information technology – Security techniques – Information security management systems – Requirements
    - ISO/IEC 27002:2005 – (re-numbered ISO17999:2005) Information technology – Security techniques – Code of practice for information security management
  - ***BC Standards***:
    - ISO/IEC 27031:2011 – Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity
    - ISO/PAS 22399:2007 – Guideline for incident preparedness and operational continuity management
    - ISO/IEC 24762:2008 – Guidelines for information and communications technology disaster recovery services
    - IWA 5:2006 – Emergency Preparedness
    - BS 25999-1:2006 – Business Continuity Management. Code of Practice
    - BS 25999-2:2007 – Specification for Business Continuity Management
    - ISO 22301:2012 – Societal security - Business continuity management systems - Requirements
    - ISO 22313:2012 – Societal security - Business continuity management systems - Guidance

3. EU-MSc PM MT

3.3. What?

- **Framework (FW)**
- **Standard (STD)**

Framework	Standard
Good practices	Best practices
Flexible	Rigid
System	Method
Best-known practices	Well-defined standard practices

http://www.cambridge.org/
http://www.pmi.org/

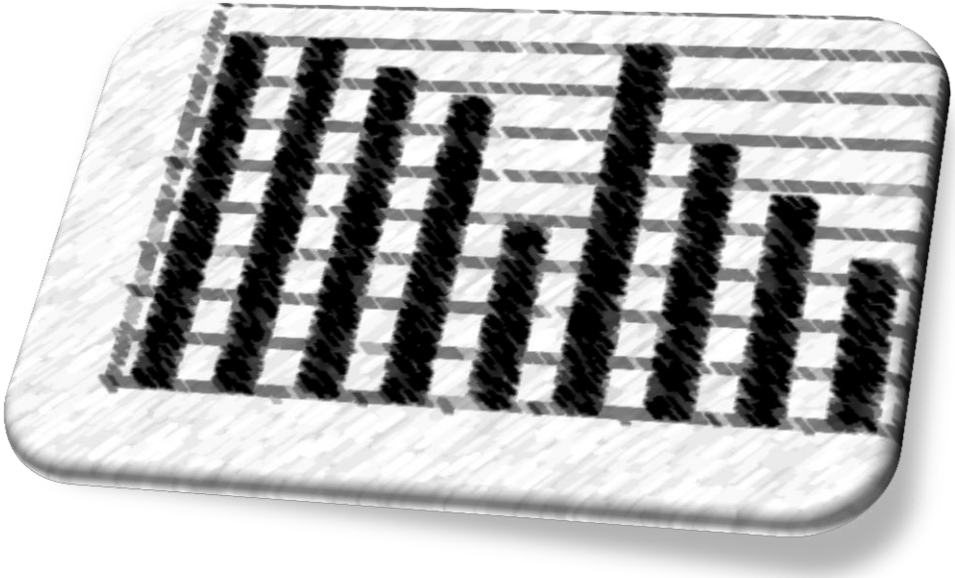
3. EU-MSc PM MT

3.4. Entities: Analysis

InfoSec AGENCIES-ASSOCIATIONS-INSTITUTIONS-BUSINESSES							
Nr.	**Abbreviation**	**Foundation Year**	**Type of Entity**	**HQ Country**	**HQ Continent**	**Language**	**Main Activity**
1	ISO/IEC JTC1	1987	AGE	US	NA	EN, FR, RU	ISM, BC
2	ISO	1946	AGE	CH	EU	EN, FR, RU	ISM, BC
3	IEC	1906	AGE	CH	EU	EN	ISM, BC
4	EUDPD	1995	AGE	BE	EU	EN	PRV
5	GDPR	2012	AGE	BE	EU	EN, DE, ES, ZH, FR, RU	PRV
6	BSI Group	1901	INS	GB	EU	EN, DE, ES, ZH, FR, RU	ISM, BC, PRV
7	DIN	1917	INS	DE	EU	EN, DE	ISM, BC
8	DSG	2000	AGE	AT	EU	EN, DE	PRV
9	BSI	1991	AGE	DE	EU	EN, DE	ISM, BC, IT
10	PMI	1969	INS	US	NA	EN	ISM
11	Cabinet Office	1916	AGE	GB	EU	EN	IT
12	APMG	1993	AGE	GB	EU	EN	IT
13	AENOR	1986	ASS	ES	EU	EN, ES	IT, ISM, BC, PRV
14	AEPD	1993	AGE	ES	EU	ES	PRV
15	ISACA	1967	ASS	US	NA	EN, DE, ES, ZH, FR	AUD, ISM, BC, PRV, IT
16	COSO	1985	ASS	US	NA	EN, ES	AUD, ISM, BC, PRV, IT
17	CISCO	1984	BUS	US	NA	EN	IT, ISM
18	IDW	1932	ASS	DE	EU	EN, DE	AUD
19	DIIR	1958	INS	DE	EU	DE	AUD
20	IAASB	1978	ASS	US	NA	EN, ES, ZH, FR	AUD
21	IIA	1941	INS	US	NA	EN	AUD, ISM
22	(ISC)²®	1988	ASS	US	NA	EN	AUD, ISM
23	AITP	1951	ASS	US	NA	EN	IT
24	ICCP	1973	INS	US	NA	EN	IT
25	IAPP	2000	ASS	US	NA	EN	PRV
26	AICPA	1887	INS	US	NA	EN	AUD
27	TheIIC	2003	INS	US	NA	EN	AUD
28	FCPAS	2005	ASS	US	NA	EN	AUD
29	ACFE	1988	ASS	US	NA	EN	AUD
30	ACCA	1904	ASS	GB	EU	EN	AUD
31	GIAC	1999	AGE	US	NA	EN	IT, ISM, AUD
32	PECB	2005	AGE	US	NA	EN	ISM, AUD, BC
33	ISO/PAS	1994	AGE	CH	EU	EN	AUD, ISM, BC, PRV, IT
34	IWA	2005	AGE	CH	EU	EN	AUD, ISM, BC, PRV, IT
35	NFPA	1896	ASS	US	NA	EN	BC
36	ANSI	1919	INS	US	NA	EN	BC, ISM
37	Standards Australia	1922	ASS	AU	OC	EN	ISM
38	ANAO	1997	AGE	AU	OC	EN	AUD
39	ASIS	1955	ASS	US	NA	EN	ISM

3. EU-MSc PM MT

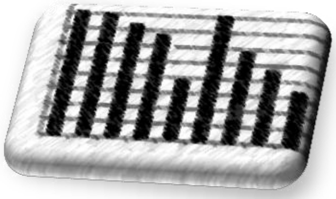
3.4. Entities: Results



STATISTICS			
	TOTAL	39	
Foundation Year	First	1887	AICPA
	Last	2012	GDPR
	TOTAL	126	
Type of Entity	AGE	15	38%
	ASS	14	36%
	INS	9	23%
	BUS	1	3%
	TOTAL	39	100%
Headquarter Country	US	20	51%
	GB	4	10%
	DE	4	10%
	ES	2	5%
	CH	4	10%
	BE	2	5%
	AT	1	3%
	AU	2	5%
	TOTAL	39	95%
Headquarter Continent	EU	17	44%
	AS	0	0%
	NA	20	51%
	SA	0	0%
	AN	0	0%
	OC	2	5%
	TOTAL	39	100%
Language	EN	37	56%
	DE	8	12%
	ES	7	11%
	ZH	4	6%
	FR	6	9%
	RU	4	6%
	TOTAL	66	100%
Main Activity	ISM	20	27%
	BC	14	19%
	AUD	17	23%
	PRV	11	15%
	IT	12	16%
	TOTAL	74	100%

3. EU-MSc PM MT

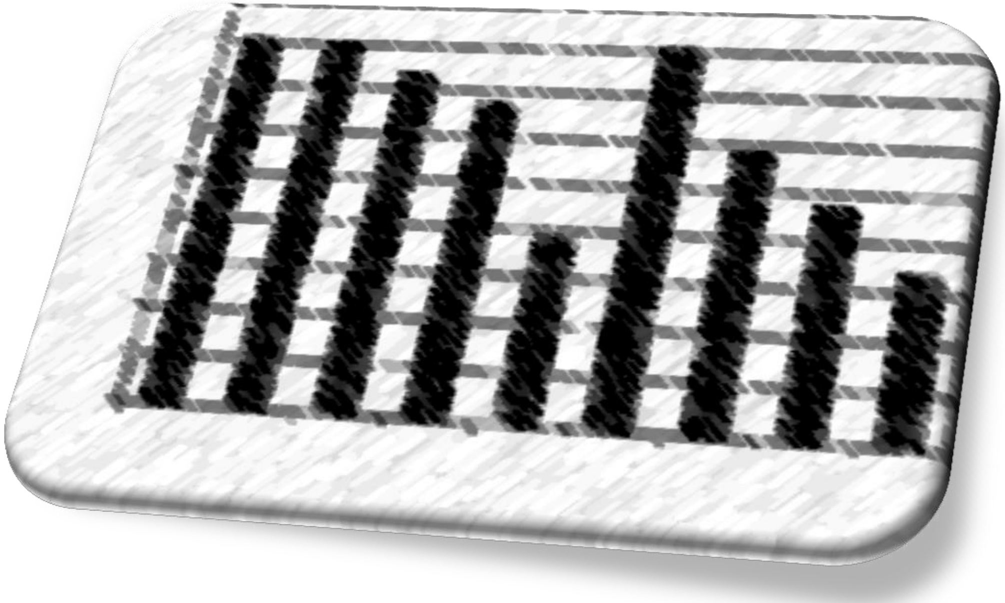
3.4. Certifications: Analysis

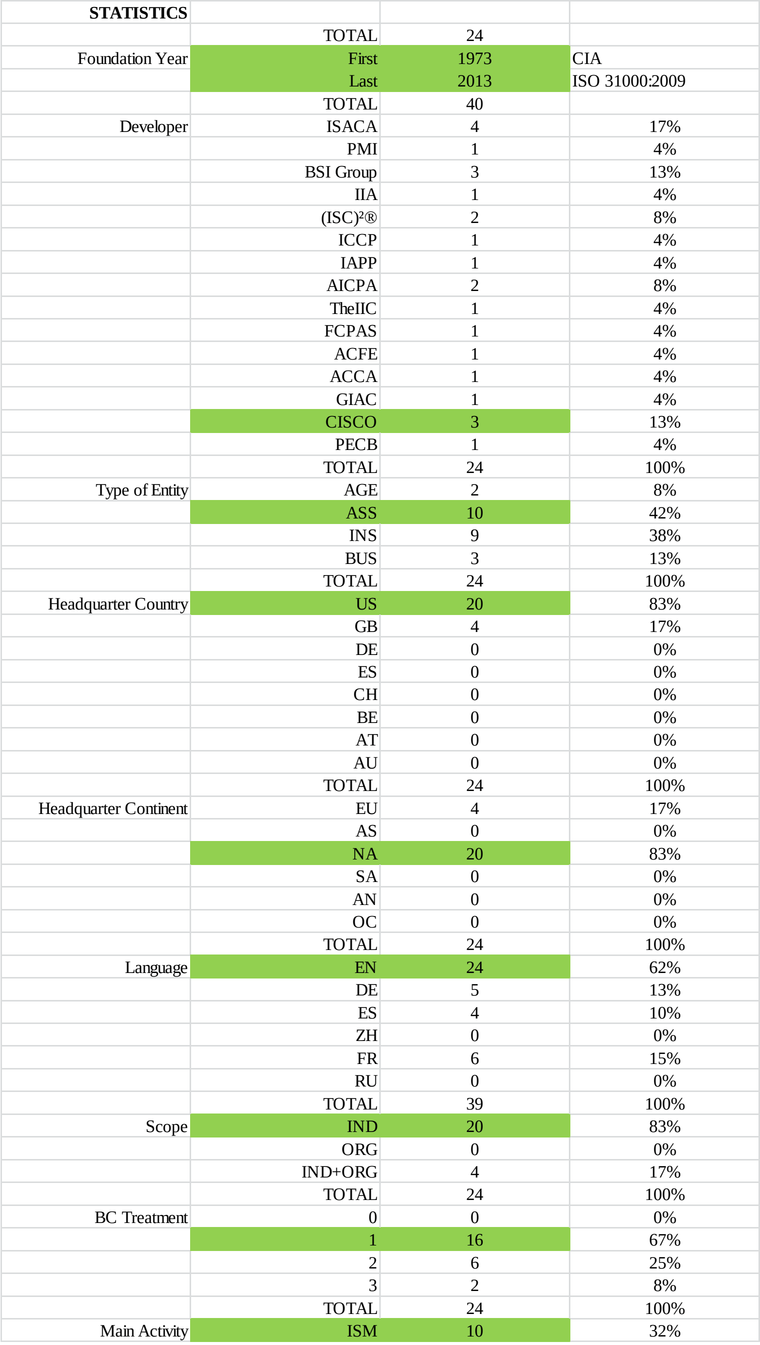


InfoSec CERTIFICATIONS										
Nr.	**Abbreviation**	**Foundation Year**	**Developer**	**Type of Entity**	**HQ Country**	**HQ Continent**	**Language**	**Scope**	**BC Treatment**	**Main Activity**
1	CISA	1978	ISACA	ASS	US	NA	EN, DE, ES, FR	IND	2	AUD
2	CISM		ISACA	ASS	US	NA	EN, DE, ES, FR	IND	2	ISM
3	CGEIT	1993	ISACA	ASS	US	NA	EN, DE, ES, FR	IND	2	ISM
4	CRISC	2011	ISACA	ASS	US	NA	EN, DE, ES, FR	IND	1	IT
5	PMI-RMP	2008	PMI	INS	US	NA	EN	IND	2	ISM
6	ISO/IEC 27001:2013	2005	BSI Group	INS	GB	EU	EN, DE, FR	IND, ORG	1	ISM
7	ISO/IEC 22301	2012	BSI Group	INS	GB	EU	EN, FR	IND, ORG	3	BC
8	ISO/IEC 22313	2012	BSI Group	INS	GB	EU	EN	IND, ORG	3	ISM, BC
9	CIA	1973	IIA	INS	US	NA	EN	IND	1	AUD
10	CAP	2005	(ISC)^{2}®	ASS	US	NA	EN	IND	1	IT
11	CCP		ICCP	INS	US	NA	EN	IND	1	IT
12	CIPP	2004	IAPP	ASS	US	NA	EN	IND	1	PRV
13	CISSP	1994	(ISC)^{2}®	ASS	US	NA	EN	IND	2	ISM, BC
14	CPA	1986	AICPA	INS	US	NA	EN	IND	1	AUD
15	CICA	2003	TheIIC	INS	US	NA	EN	IND	1	AUD
16	FCPA	2005	FCPAS	ASS	US	NA	EN	IND	1	AUD
17	CFA		ACFE	ASS	US	NA	EN	IND	1	AUD
18	CCA	1996	ACCA	ASS	GB	EU	EN	IND	1	AUD
19	GSNA		GIAC	AGE	US	NA	EN	IND	1	AUD
20	CITP		AICPA	INS	US	NA	EN	IND	1	AUD
21	CCNA Security		CISCO	BUS	US	NA	EN	IND	1	IT, ISM
22	CCNP Security		CISCO	BUS	US	NA	EN	IND	1	IT, ISM
23	CCIE Security		CISCO	BUS	US	NA	EN	IND	1	IT, ISM
24	ISO 31000:2009	2013	PECB	AGE	US	NA	EN	IND, ORG	2	ISM, AUD, BC

3. EU-MSc PM MT

3.4. Certifications: Results





STATISTICS			
	TOTAL	24	
Foundation Year	First	1973	CIA
	Last	2013	ISO 31000:2009
	TOTAL	40	
Developer	ISACA	4	17%
	PMI	1	4%
	BSI Group	3	13%
	IIA	1	4%
	(ISC)²®	2	8%
	ICCP	1	4%
	IAPP	1	4%
	AICPA	2	8%
	TheIIC	1	4%
	FCPAS	1	4%
	ACFE	1	4%
	ACCA	1	4%
	GIAC	1	4%
	CISCO	3	13%
	PECB	1	4%
	TOTAL	24	100%
Type of Entity	AGE	2	8%
	ASS	10	42%
	INS	9	38%
	BUS	3	13%
	TOTAL	24	100%
Headquarter Country	US	20	83%
	GB	4	17%
	DE	0	0%
	ES	0	0%
	CH	0	0%
	BE	0	0%
	AT	0	0%
	AU	0	0%
	TOTAL	24	100%
Headquarter Continent	EU	4	17%
	AS	0	0%
	NA	20	83%
	SA	0	0%
	AN	0	0%
	OC	0	0%
	TOTAL	24	100%
Language	EN	24	62%
	DE	5	13%
	ES	4	10%
	ZH	0	0%
	FR	6	15%
	RU	0	0%
	TOTAL	39	100%
Scope	IND	20	83%
	ORG	0	0%
	IND+ORG	4	17%
	TOTAL	24	100%
BC Treatment	0	0	0%
	1	16	67%
	2	6	25%
	3	2	8%
	TOTAL	24	100%
Main Activity	ISM	10	32%

3. EU-MSc PM MT

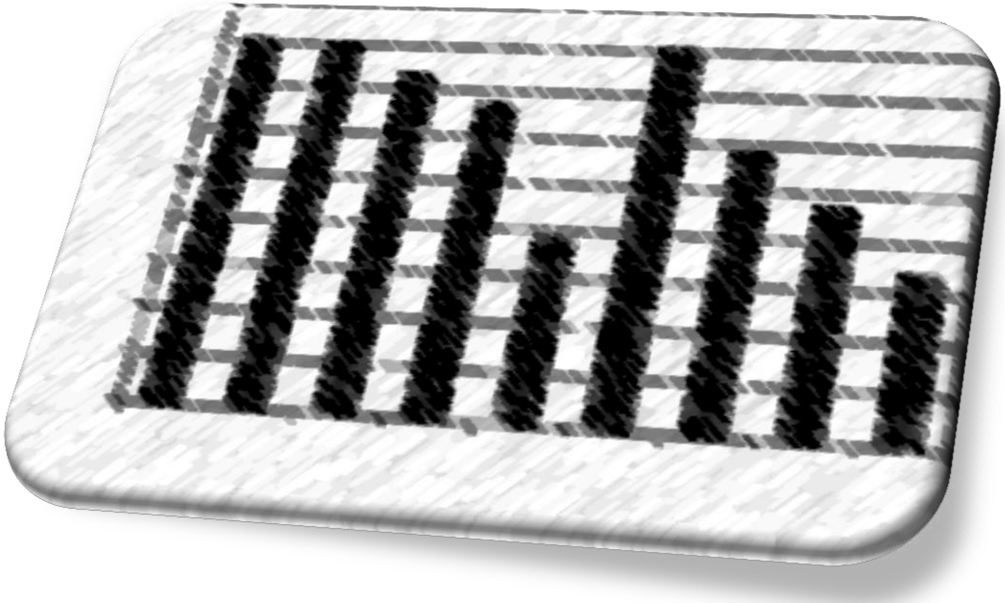
3.4. Frameworks: Analysis

BC & FRAMEWORKS							
Nr.	ID	First Version	First Version Year	Last Version	Last Version Year	Developer	Type of Entity
1	PMBOK	1st Edition	1996	5th Edition	2013	PMI	INS
2	ITIL	v1	2001	2011 Edition	2011	Cabinet Office	AGE
3	COBIT	1s Edition	1996	COBIT 5	2012	ISACA	ASS
4	ValIT	v.1.0	2006	v.2.0	2008	ISACA	ASS
5	RiskIT	v.1.0	2009	v.1.0	2009	ISACA	ASS
6	COSO Model of Internal Control	1992	1992	2012	2011	COSO	ASS
7	BSI-Standard 100-1	v.1.0	2008	v.1.0	2008	BSI	AGE

BC & FRAMEWORKS								
Nr.	ID	HQ Country	HQ Continent	Language	Scope	BC Treatment	Descriptor	Main Activity
1	PMBOK	US	NA	EN, DE, ES, ZH, FR, RU	IND	1	GLO, GUI	ISM
2	ITIL	GB	EU	EN	IND	1	GUI	IT
3	COBIT	US	NA	EN	ORG	2	GLO, GUI	ISM
4	ValIT	US	NA	EN	ORG	2	GLO, GUI	ISM
5	RiskIT	US	NA	EN	ORG	2	GLO, GUI	ISM
6	COSO Model of Internal Control	US	NA	EN, ES	IND, ORG	2	AUD, ISM	AUD, ISM, BC, PRV, IT
7	BSI-Standard 100-1	DE	EU	EN, DE	IND, ORG	2	GUI	AUD

3. EU-MSc PM MT

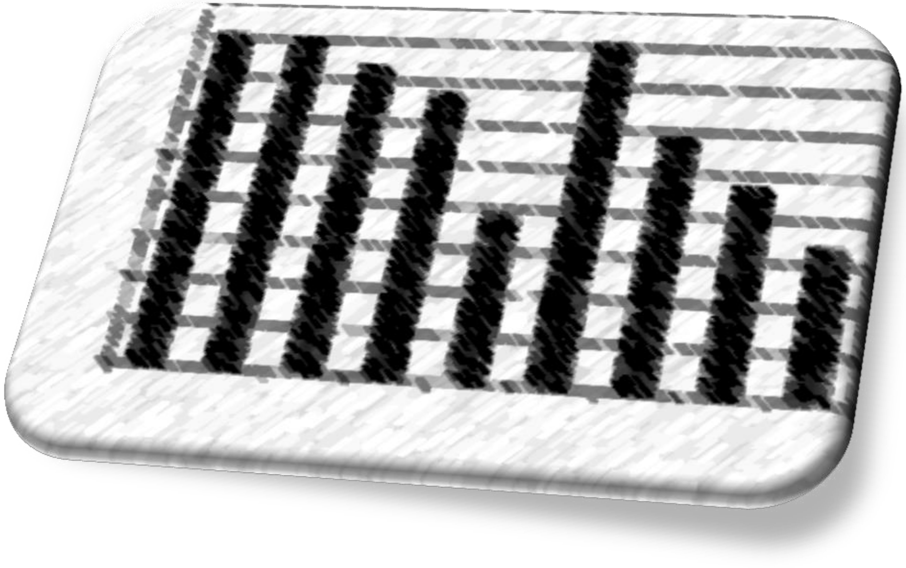
3.4. Frameworks: Results



STATISTICS			
	TOTAL	7	
First Version Year	First	1992	COSO Model of Internal Control
	Last	2009	RiskIT
	TOTAL	21	
Last Version Year	First	2008	ValIT, BSI-Standard 100-1
	Last	2013	PMBOK
	TOTAL	5	
Developer	PMI	1	14%
	Cabinet Office	1	14%
	ISACA	3	43%
	COSO	1	14%
	BSI	1	14%
	TOTAL	7	100%
Type of Entity	AGE	2	29%
	ASS	4	57%
	INS	1	14%
	BUS	0	0%
	TOTAL	7	100%
Headquarter Country	US	5	71%
	GB	1	14%
	DE	1	14%
	ES	0	0%
	CH	0	0%
	BE	0	0%
	AT	0	0%
	AU	0	0%
	TOTAL	7	100%
Headquarter Continent	EU	2	29%
	AS	0	0%
	NA	5	71%
	SA	0	0%
	AN	0	0%
	OC	0	0%
	TOTAL	7	100%

3. EU-MSc PM MT

3.4. Frameworks: Results



Language	EN	7	50%
	DE	2	14%
	ES	2	14%
	ZH	1	7%
	FR	1	7%
	RU	1	7%
	TOTAL	14	100%
Inherited	Yes	3	43%
	No	4	57%
	TOTAL	7	100%
Scope	IND	2	29%
	ORG	3	43%
	IND+ORG	2	29%
	TOTAL	7	100%
BC Treatment	0	0	0%
	1	2	29%
	2	5	71%
	3	0	0%
	TOTAL	7	100%
Descriptor	GLO	4	40%
	REQ	0	0%
	GUI	6	60%
	BPR	0	0%
	TCH	0	0%
	REF	0	0%
	TOTAL	10	100%
Main Activity	ISM	5	45%
	BC	1	9%
	AUD	2	18%
	PRV	1	9%
	IT	2	18%
	TOTAL	11	100%

3. EU-MSc PM MT

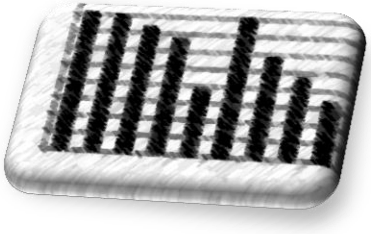
3.4. Standards: Analysis (1/2)

BC & STANDARDS

Nr.	ID	First Version	First Version Year	Last Version	Last Version Year	Developer	Type of Entity
1	ISO/IEC 20000-1:2011	ISO/IEC 20000-1:2005	2005	ISO/IEC 20000-1:2011	2011	ISO/IEC	AGE
2	ISO/IEC 20000-2:2012	ISO/IEC 20000-2:2005	2005	ISO/IEC 20000-2:2012	2012	ISO/IEC	AGE
3	ISO/IEC 20000-3:2012	ISO/IEC 20000-3:2009	2009			ISO/IEC	AGE
4	ISO/IEC 20000-4:2010	ISO/IEC 20000-4:2010	2010			ISO/IEC	AGE
5	ISO/IEC 20000-5:2010	ISO/IEC 20000-5:2010	2010			ISO/IEC	AGE
6	ISO 31000:2009	ISO 31000:2009	2009			ISO	AGE
7	ISO/IEC 31010:2009	ISO/IEC 31010:2009	2009			ISO/IEC	AGE
8	ISO Guide 73:2009	ISO Guide 73:2009	2009			ISO	AGE
9	ISO/IEC 27001:2013	ISO/IEC 27001:2005	2005	ISO/IEC 27001:2013	2013	ISO/IEC	AGE
10	ISO/IEC 27002:2005	ISO/IEC 27002:2005	2005			ISO/IEC	AGE
11	ISO/IEC 27031:2011	ISO/IEC 27031:2011	2011			ISO/IEC	AGE
12	ISO/PAS 22399:2007	ISO/PAS 22399:2007	2007			ISO/PAS	AGE
13	ISO/IEC 24762:2008	ISO/IEC 24762:2008	2008			ISO/IEC	AGE
14	IWA 5:2006	IWA 5:2006	2006			ISO	AGE
15	BS 25999-1:2006	BS 25999-1:2006	2006			BSI Group	INS
16	BS 25999-2:2007	BS 25999-2:2007	2007			BSI Group	INS
17	ISO 22301:2012	ISO 22301:2012	2012			ISO	AGE
18	ISO 22313:2012	ISO 22313:2012	2012			ISO	AGE
19	BSI-Standard 100-1	v.1.0	2005	v.1.5	2008	BSI	AGE
20	BSI-Standard 100-2	v.1.0	2005	v.2.0	2008	BSI	AGE
21	BSI-Standard 100-3	v.1.0	2004	v.2.5	2008	BSI	AGE
22	BSI-Standard 100-4	v.1.0	2008			BSI	AGE
23	ISO/IEC 27005:2011	ISO/IEC 27005:2008	2008	ISO/IEC 27005:2011	2011	ISO/IEC JTC1	AGE
24	NFPA 1600:2013	NFPA 1600:1995	1995	NFPA 1600:2013	2013	NFPA	ASS
25	ASIS/BSI BCM.01-2010	ASIS/BSI BCM.01-2010	2010			ANSI, ASIS	ASS, INS
26	ANSI/ASIS SPC.1-2009	ANSI/ASIS SPC.1-2009	2009			ANSI, ASIS	ASS, INS
27	HB 292-2006	HB 292-2006	2006			Standards Australia	ASS
28	HB 293-2006	HB 293-2006	2006			Standards Australia	ASS

3. EU-MSc PM MT

3.4. Standards: Analysis (2/2)

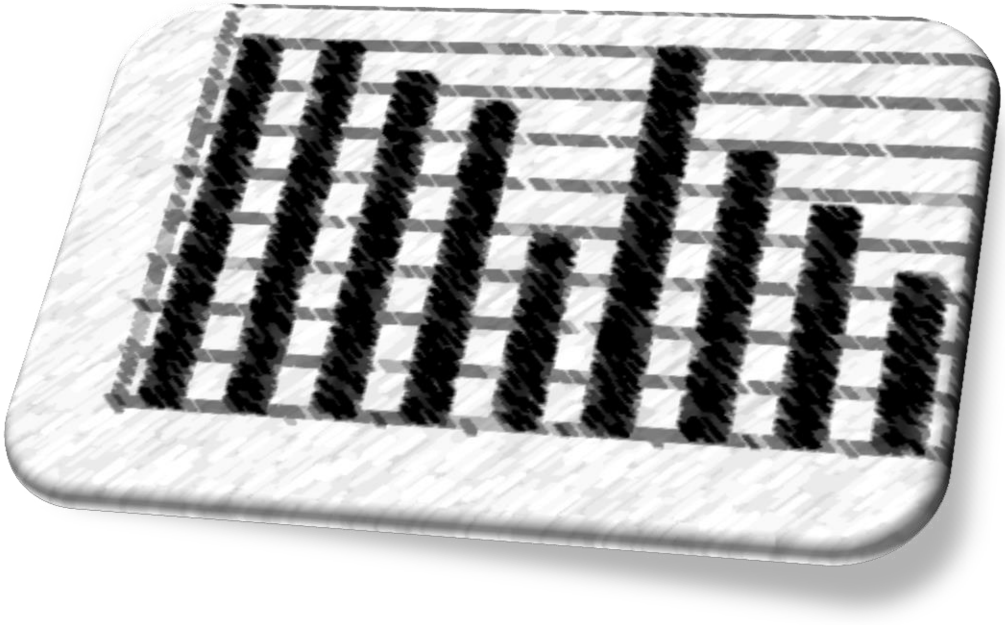


BC & STANDARDS

Nr.	ID	HQ Country	HQ Continent	Language	Inherited	Scope	BC Treatment	Descriptor	Main Activity
1	ISO/IEC 20000-1:2011	US	NA	EN, FR, RU	ITIL, BS 15000	IND, ORG	1	REQ	ISM
2	ISO/IEC 20000-2:2012	US	NA	EN, FR, RU	ITIL, BS 15000	IND, ORG	1	GUI	ISM
3	ISO/IEC 20000-3:2012	US	NA	EN, FR, RU	ITIL, BS 15000	IND, ORG	1	GUI	ISM
4	ISO/IEC 20000-4:2010	US	NA	EN, FR, RU	ITIL, BS 15000	IND, ORG	1	REF	ISM
5	ISO/IEC 20000-5:2010	US	NA	EN, FR, RU	ITIL, BS 15000	IND, ORG	1	GUI	ISM
6	ISO 31000:2009	CH	EU	EN, FR, RU		IND, ORG	1	GUI	ISM
7	ISO/IEC 31010:2009	US	NA	EN, FR, RU	ISO 31000:2009	IND, ORG	1	TCH	ISM
8	ISO Guide 73:2009	CH	EU	EN, FR, RU	ISO 31000:2009	IND, ORG	1	GLO	ISM
9	ISO/IEC 27001:2013	US	NA	EN, FR, RU		IND, ORG	1	REQ	ISM
10	ISO/IEC 27002:2005	US	NA	EN, FR, RU	BS 7799	IND	1	BPR	ISM
11	ISO/IEC 27031:2011	US	NA	EN, FR, RU	ISO/IEC 27001:2005	ORG	3	GUI	BC
12	ISO/PAS 22399:2007	CH	EU	EN		ORG	3	GUI	BC
13	ISO/IEC 24762:2008	US	NA	EN, FR, RU		ORG	3	GUI	IT
14	IWA 5:2006	CH	EU	EN		IND, ORG	3	REQ	BC
15	BS 25999-1:2006	GB	EU	EN, DE, ES, ZH, FR, RU		IND, ORG	3	BPR	BC
16	BS 25999-2:2007	GB	EU	EN, DE, ES, ZH, FR, RU		IND, ORG	3	REF	BC
17	ISO 22301:2012	CH	EU	EN, FR, RU	BS 25999-2:2007	IND, ORG	3	REQ	BC
18	ISO 22313:2012	CH	EU	EN, FR, RU		ORG	3	GUI	BC
19	BSI-Standard 100-1	DE	EU	EN, DE		ORG	1	REF	ISM
20	BSI-Standard 100-2	DE	EU	EN, DE	ISO/IEC 2700X	ORG	1	GUI	ISM
21	BSI-Standard 100-3	DE	EU	EN, DE		ORG	2	REQ	ISM
22	BSI-Standard 100-4	DE	EU	EN, DE		ORG	3	GUI	BC
23	ISO/IEC 27005:2011	US	NA	EN, FR, RU		IND, ORG	1	TCH	IT, ISM
24	NFPA 1600:2013	US	NA	EN	NFPA 1600:1995	ORG	3	GUI	BC
25	ASIS/BSI BCM.01-2010	US	NA	EN	BS 25999	ORG	3	REQ, GUI	BC
26	ANSI/ASIS SPC.1-2009	US	NA	EN		IND	3	REQ, GUI	BC
27	HB 292-2006	US	NA	EN		IND	3	GUI	BC
28	HB 293-2006	US	NA	EN		IND	3	GUI	BC

3. EU-MSc PM MT

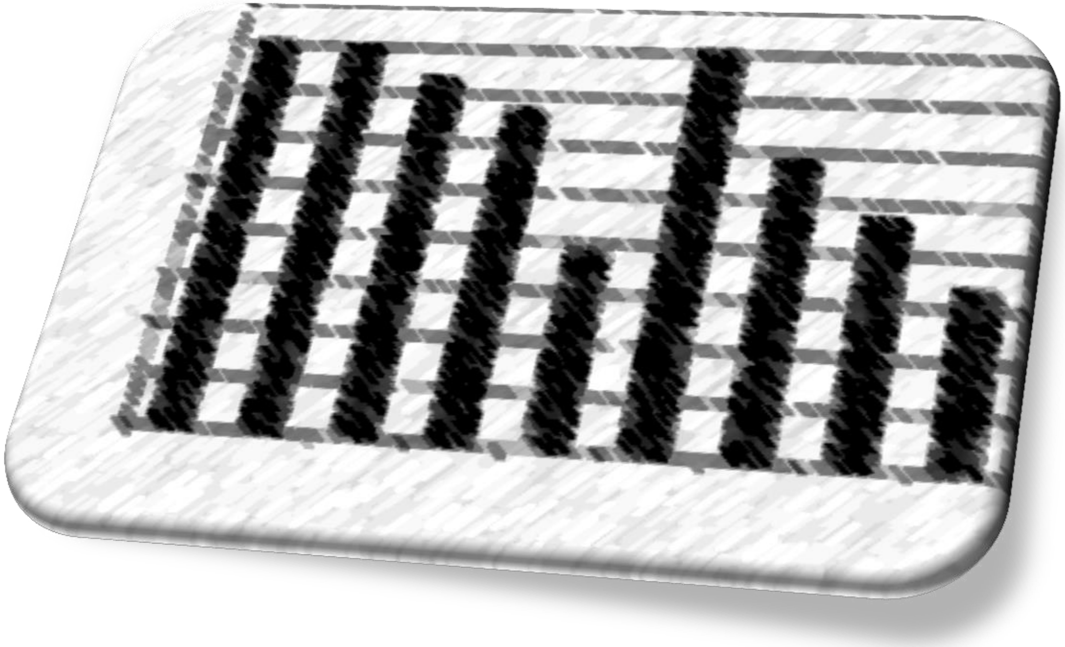
3.4. Standards: Results (1/2)



STATISTICS			
	TOTAL	28	
First Version Year	First	1995	NFPA 1600:2013
	Last	2012	ISO 22301:2012, ISO 22313:2012
	TOTAL	18	
Last Version Year	First	2008	BSI-Standard 100-1, BSI-Standard 100-2, BSI-Standard 100-3
	Last	2013	ISO/IEC 27001:2013, NFPA 1600:2013
	TOTAL	5	
Developer	ISO/IEC	11	25%
	ISO	17	39%
	BSI Group	2	5%
	NFPA	1	2%
	ISO/IEC JTC1	1	2%
	ANSI	2	5%
	ASIS	2	5%
	Standards Australia	2	5%
	BSI	6	14%
	TOTAL	44	100%
Type of Entity	AGE	21	81%
	ASS	3	12%
	INS	2	8%
	BUS	0	0%
	TOTAL	26	100%
Headquarter Country	US	16	57%
	GB	2	7%
	DE	4	14%
	ES	0	0%
	CH	6	21%
	BE	0	0%
	AT	0	0%
	AU	0	0%
	TOTAL	28	100%
Headquarter Continent	EU	12	43%
	AS	0	0%
	NA	16	57%
	SA	0	0%
	AN	0	0%
	OC	0	0%
	TOTAL	28	100%

3. EU-MSc PM MT

3.4. Standards: Results (2/2)



Language	EN	28	39%
	DE	6	8%
	ES	2	3%
	ZH	2	3%
	FR	17	24%
	RU	17	24%
	TOTAL	72	100%
Inherited	Yes	13	46%
	No	15	54%
	TOTAL	28	100%
Scope	IND	4	14%
	ORG	10	36%
	IND+ORG	14	50%
	TOTAL	28	100%
BC Treatment	0	0	0%
	1	13	46%
	2	1	4%
	3	14	50%
	TOTAL	28	100%
Descriptor	GLO	1	3%
	REQ	7	23%
	GUI	15	50%
	BPR	2	7%
	TCH	2	7%
	REF	3	10%
	TOTAL	30	100%
Main Activity	ISM	14	48%
	BC	13	45%
	AUD	0	0%
	PRV	0	0%
	IT	2	7%
	TOTAL	29	100%

3. EU-MSc PM MT

3.5. Conclusion: Results Analysis

- **Extense documentation and information** about: InfoSec, BC, and AUD. **Mostly private**.
- **Analysis**: 39 Entities, 24 Certifications, 7 Frameworks, and 28 Standards.
- Conclusions from **Results**:
  - High number of STD relatively “new” (18 years)
  - >% FW by ASS; >% STD by AGE
  - >% Certifications by: ISACA, BSI Group, CISCO
  - >% FW by: ISACA, BSI
  - >% STD by: ISO, ISO/IEC, BSI
  - >% HQ Country by US
  - >% HQ Continent by NA +/- EU
  - >% Language is EN. DE and ES increasing
  - >% Scope: Cert=IND; FW=ORG, STD=IND+ORG
  - >% BC Treatment: Cert=Related; FW=Considerable; STD=Total
  - >% Descriptors: FW=GUI+GLO; STD=GUI
  - Main Activity: BC: Ent=19%; Cert=13%; FW=9%; STD=45%

3. EU-MSc PM MT

3.5. Conclusion: BC STD Advantages & Disadvantages

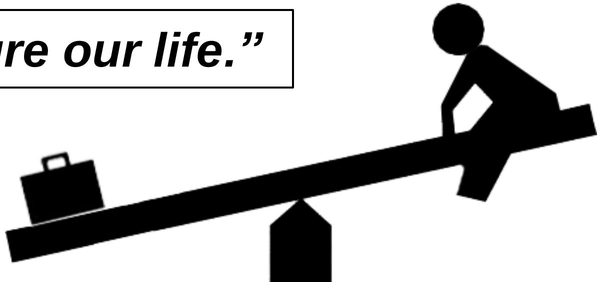
BC STD Advantages	BC STD Disadvantages
Maximize Q' and Efficiency	Does not guarantee superior Q', STD just certifies the company
Flexibility during disruption	Force to change stablished methods
Competitive advantage	Reduce productivity by forcing unnecessary actions
Ensure safety & security: reduce risk	Do not prevent bugs
Organisational improvement	Required investment of: money, time, paperwork
Continuous internal improvement via audits	Excess of information: it is better to be brief, clear and concise
Legal & Regulatory compliance	Concepts repetition
Cost savings	Economical interest
Maintain optimum client delivery levels	Sparse resources
Strengthen your internal management	STD Implementation reduces creativity
Reputational management	
Specialization of BC to the concrete area each standard is applied	
Business and Job opportunities	
Support from one Standards/Frameworks to the others	

3. EU-MSc PM MT

3.5. Conclusion: Effective & efficient progress

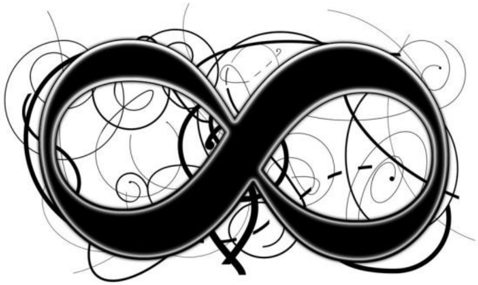
- **Optimization:** BCM aims must meet interdependence and interdisciplinary.
- **New solution:** globalized organization (like or under ISO) to develop and provide: certifications, STD, research, methods, tools, and techniques.
- **Prospection**: research on AUD-DF mechanisms to effectively and efficiently assess CI safety and security investment.
- **Opportunity:** third party involved entities procedures implementation, execution and development to ensure InfoSec and BC.

"Imperative necessity of BC: safeguard and secure our life."



Index

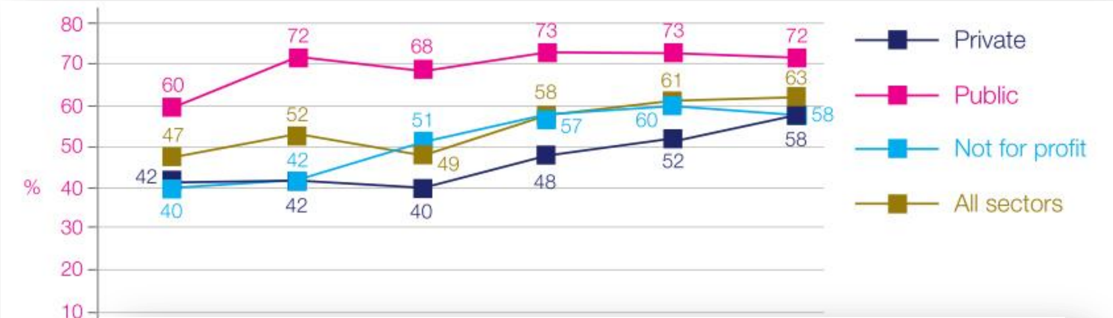
1. Introduction
2. MSc InfoSec MT
3. EU-MSc PM MT
4. ***Research***
    1. **Statistics**
    2. **BC SW**
    3. **Requirements: Present-Future**

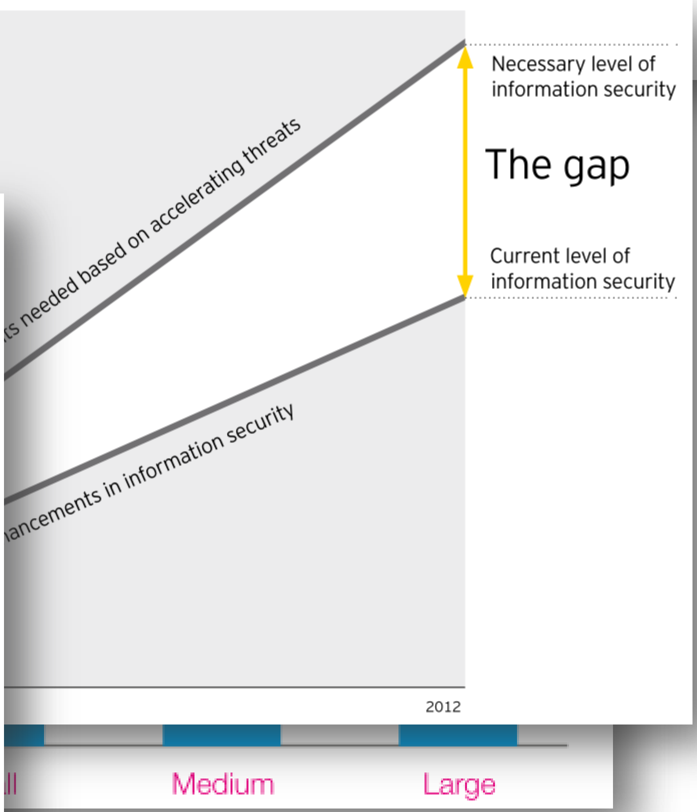


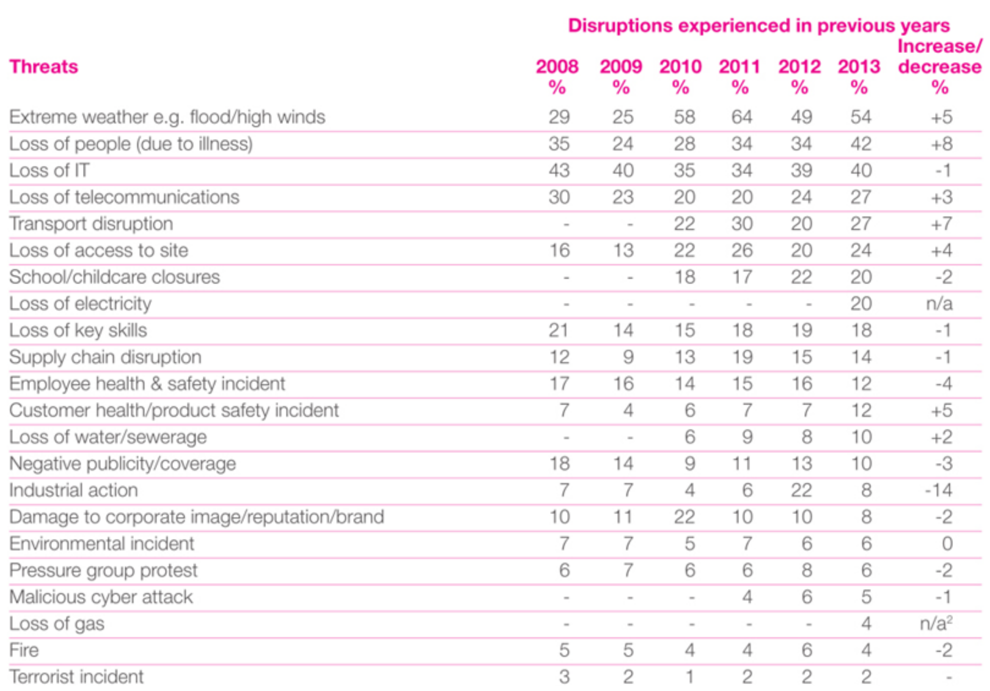
4. Research

4.1. Statistics

- ORG with BCM
- ORG with BCP by Size
- The gap
- Sources of disruption




ts needed based on accelerating threats
ancements in information security
Necessary level of information security
The gap
Current level of information security
2012
80
70
ll
Medium
Large



Threats	Disruptions experienced in previous years						
	2008 %	2009 %	2010 %	2011 %	2012 %	2013 %	Increase/ decrease %
Extreme weather e.g. flood/high winds	29	25	58	64	49	54	+5
Loss of people (due to illness)	35	24	28	34	34	42	+8
Loss of IT	43	40	35	34	39	40	-1
Loss of telecommunications	30	23	20	20	24	27	+3
Transport disruption	-	-	22	30	20	27	+7
Loss of access to site	16	13	22	26	20	24	+4
School/childcare closures	-	-	18	17	22	20	-2
Loss of electricity	-	-	-	-	-	20	n/a
Loss of key skills	21	14	15	18	19	18	-1
Supply chain disruption	12	9	13	19	15	14	-1
Employee health & safety incident	17	16	14	15	16	12	-4
Customer health/product safety incident	7	4	6	7	7	12	+5
Loss of water/sewerage	-	-	6	9	8	10	+2
Negative publicity/coverage	18	14	9	11	13	10	-3
Industrial action	7	7	4	6	22	8	-14
Damage to corporate image/reputation/brand	10	11	22	10	10	8	-2
Environmental incident	7	7	5	7	6	6	0
Pressure group protest	6	7	6	6	8	6	-2
Malicious cyber attack	-	-	-	4	6	5	-1
Loss of gas	-	-	-	-	-	4	n/a^{2}
Fire	5	5	4	4	6	4	-2
Terrorist incident	3	2	1	2	2	2	-

Chartered Management Institute (CMI), "Weathering the Storm: the 2013 Business Continuity Management Survey," CMI, London (United Kingdom), 2013.

4. Research

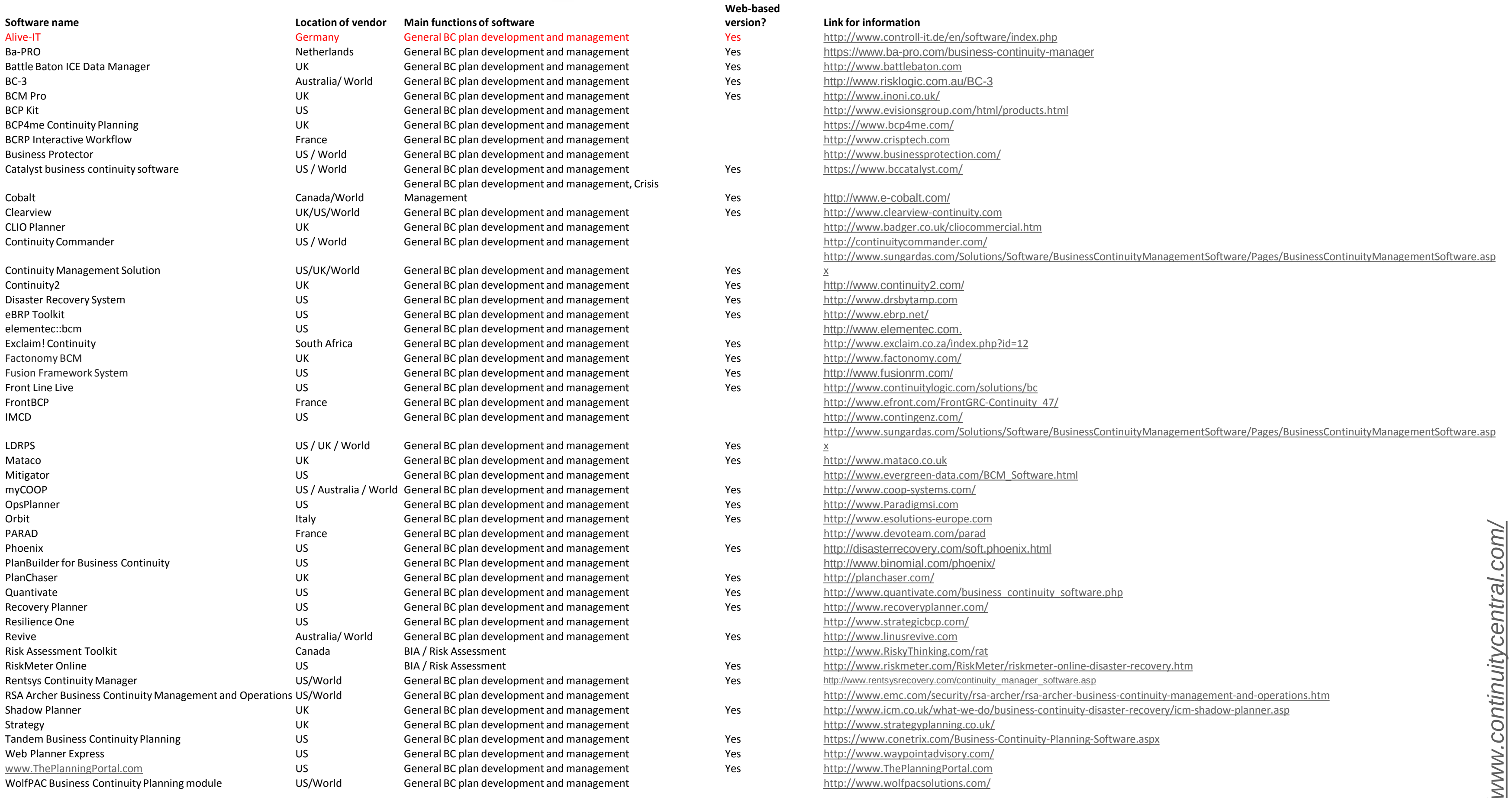
4.1. BC SW

Alive-IT

http://bcm-inv.enisa.europa.eu/tools/t_alive.html

http://www.controll-it.de/de/home-de

Business continuity software



Software name	Location of vendor	Main functions of software	Web-based version?	Link for information
Alive-IT	Germany	General BC plan development and management	Yes	http://www.controll-it.de/en/software/index.php
Ba-PRO	Netherlands	General BC plan development and management	Yes	https://www.ba-pro.com/business-continuity-manager
Battle Baton ICE Data Manager	UK	General BC plan development and management	Yes	http://www.battlebaton.com
BC-3	Australia/ World	General BC plan development and management	Yes	http://www.risklogic.com.au/BC-3
BCM Pro	UK	General BC plan development and management	Yes	http://www.inoni.co.uk/
BCP Kit	US	General BC plan development and management		http://www.evisionsgroup.com/html/products.html
BCP4me Continuity Planning	UK	General BC plan development and management		https://www.bcp4me.com/
BCRP Interactive Workflow	France	General BC plan development and management		http://www.crisptech.com
Business Protector	US / World	General BC plan development and management		http://www.businessprotection.com/
Catalyst business continuity software	US / World	General BC plan development and management	Yes	https://www.bccatalyst.com/
Cobalt	Canada/World	General BC plan development and management, Crisis Management	Yes	http://www.e-cobalt.com/
Clearview	UK/US/World	General BC plan development and management	Yes	http://www.clearview-continuity.com
CLIO Planner	UK	General BC plan development and management		http://www.badger.co.uk/cliocommercial.htm
Continuity Commander	US / World	General BC plan development and management		http://continuitycommander.com/
Continuity Management Solution	US/UK/World	General BC plan development and management	Yes	http://www.sungardas.com/Solutions/Software/BusinessContinuityManagementSoftware/Pages/BusinessContinuityManagementSoftware.aspx
Continuity2	UK	General BC plan development and management	Yes	http://www.continuity2.com/
Disaster Recovery System	US	General BC plan development and management	Yes	http://www.drsbytamp.com
eBRP Toolkit	US	General BC plan development and management	Yes	http://www.ebrp.net/
elementec::bcm	US	General BC plan development and management		http://www.elementec.com.
Exclaim! Continuity	South Africa	General BC plan development and management	Yes	http://www.exclaim.co.za/index.php?id=12
Factonomy BCM	UK	General BC plan development and management	Yes	http://www.factonomy.com/
Fusion Framework System	US	General BC plan development and management	Yes	http://www.fusionrm.com/
Front Line Live	US	General BC plan development and management	Yes	http://www.continuitylogic.com/solutions/bc
FrontBCP	France	General BC plan development and management		http://www.efront.com/FrontGRC-Continuity_47/
IMCD	US	General BC plan development and management		http://www.contingenz.com/
LDRPS	US / UK / World	General BC plan development and management	Yes	http://www.sungardas.com/Solutions/Software/BusinessContinuityManagementSoftware/Pages/BusinessContinuityManagementSoftware.aspx
Mataco	UK	General BC plan development and management	Yes	http://www.mataco.co.uk
Mitigator	US	General BC plan development and management		http://www.evergreen-data.com/BCM_Software.html
myCOOP	US / Australia / World	General BC plan development and management	Yes	http://www.coop-systems.com/
OpsPlanner	US	General BC plan development and management	Yes	http://www.Paradigmsi.com
Orbit	Italy	General BC plan development and management	Yes	http://www.esolutions-europe.com
PARAD	France	General BC plan development and management		http://www.devoteam.com/parad
Phoenix	US	General BC plan development and management	Yes	http://disasterrecovery.com/soft.phoenix.html
PlanBuilder for Business Continuity	US	General BC Plan development and management		http://www.binomial.com/phoenix/
PlanChaser	UK	General BC plan development and management	Yes	http://planchaser.com/
Quantivate	US	General BC plan development and management	Yes	http://www.quantivate.com/business_continuity_software.php
Recovery Planner	US	General BC plan development and management	Yes	http://www.recoveryplanner.com/
Resilience One	US	General BC plan development and management		http://www.strategicbcp.com/
Revive	Australia/ World	General BC plan development and management	Yes	http://www.linusrevive.com
Risk Assessment Toolkit	Canada	BIA / Risk Assessment		http://www.RiskyThinking.com/rat
RiskMeter Online	US	BIA / Risk Assessment	Yes	http://www.riskmeter.com/RiskMeter/riskmeter-online-disaster-recovery.htm
Rentsys Continuity Manager	US/World	General BC plan development and management	Yes	http://www.rentsysrecovery.com/continuity_manager_software.asp
RSA Archer Business Continuity Management and Operations	US/World	General BC plan development and management		http://www.emc.com/security/rsa-archer/rsa-archer-business-continuity-management-and-operations.htm
Shadow Planner	UK	General BC plan development and management	Yes	http://www.icm.co.uk/what-we-do/business-continuity-disaster-recovery/icm-shadow-planner.asp
Strategy	UK	General BC plan development and management		http://www.strategyplanning.co.uk/
Tandem Business Continuity Planning	US	General BC plan development and management	Yes	https://www.conetrix.com/Business-Continuity-Planning-Software.aspx
Web Planner Express	US	General BC plan development and management	Yes	http://www.waypointadvisory.com/
www.ThePlanningPortal.com	US	General BC plan development and management	Yes	http://www.ThePlanningPortal.com
WolfPAC Business Continuity Planning module	US/World	General BC plan development and management		http://www.wolfpacsolutions.com/

http://www.continuitycentral.com/

http://bcm-inv.enisa.europa.eu/tools/t_alive.html

http://www.controll-it.de/de/home-de

4. Research

4.1. Requirements: Present & Future

- BC is relative new (BS 25999-1:2006)
- BC Mechanisms: Methods, Tools & Techniques
  - Preventive
  - Mitigation
  - Recovery

- Academic & Professional // Research
- Business & IT = Single body
- Gap:
  - Digital Forensics Audit & BC interests collide in CI
  - MD, Infosec & BC
  - BYOD
  - CI → Safety & Security
  - Projects: SAFEST, Peeroskop, Alive-IT, …

7. References

- Project Management Institute, Inc., A guide to the project management body of knowledge (PMBOK ® guide). -- Fifth edition, Pennsylvania: Project Management Institute, Inc., 2013.
- International Orgamization for Standardization (ISO), “ISO/DIS 22313:2012 Societal security -- Business continuity management systems -- Guidance,” ISO, Geneva (Switzerland), 2012.
- A. M. Suduc, M. Bîzoi and F. G. FILIP, “Audit for Information Systems Security,” *Informatica Economică,* vol. 14, no. 1, pp. 43-48, 2010.
- Bundesamt für Sicherheit in der Informationstechnik, “Information security audit (IS audit) - A guideline for IS audits based on IT-Grundschutz,” German Federal Office for Information Security, Bonn, 2008.
- Information Systems Audit and Control Association (ISACA), Certified Information Systems Auditor: CISA Review Manual, Illinois (USA): ISACA, 2011.
- Office of Government Commerce, “ITIL: The Basics,” APM Group Limited, (United Kingdom), 2010.
- R. Willison and M. Siponen, “Information security management standards: Problems and solutions,” *Information & Management,* vol. 46, p. 267–270, 2009.
- V. Morabito and F. Arduini, “Information Technology Business Continuity,” *Communications of the Association for Computing Machinery (ACM),* vol. 53, no. 3, pp. 121-125, March 2010.
- M. Spremić, “Standards and Frameworks for Information System,” in *Proceedings of the World Congress on Engineering 2011*, London, 2011.
- M. G. Dequae, “The cyber challenge,” *FERMA,* pp. 8-9, 2013.
- Business Continuity Institute (BCI), “Horizon Scan 2012,” BCI, Berkshire (United Kingdom), 2012.
- Symantec, “Internet Security Threat Report 2013,” Symantec, California (USA), 2013.
- Business Continuity Institute (BCI), “Horizon Scan 2013,” BCI, Berkshire (United Kingdom), 2013.
- H. Korkmazyürek and K. Hazır, “Crisis Management and Business Continuity Management: A Five-Dimension Model for Differentiating the relevant concepts,” *International Conference on Business, Economics and Management,* pp. 1-8, 2010.
- K. Roebuck, Business continuity and disaster recovery, (UK): Emereo Pty Limited, 2011.
- S. P. Low, J. Liu and S. Sio, “Business continuity management in large construction companies in Singapore,” *Disaster Prevention and Management,* vol. 19, no. 2, pp. 219-232, 2010.
- N. W. Wong, “The strategic skills of business continuity managers: putting business continuity management into corporate long-term planning,” *Journal of Business Continuity & Emergency Planning,* vol. 4, no. 1, pp. 62-68, 2009.
- K. Randeree, K. A. Mahal and A. Narwani, “A business continuity management maturity model for the UAE banking sector,” *Business Process Management Journal,* vol. 18, no. 3, pp. 472-492, 2012.
- …

Questions

Copyright

- In this final work names, trademarks, signs and so on can be registered trademarks of their respective companies.
- All in this work uses pictures are a copyright © of the producer.

©

Copyleft