EURid approach to contingencies

ICANN Sydney, ccNSO meeting, 24 June 2009

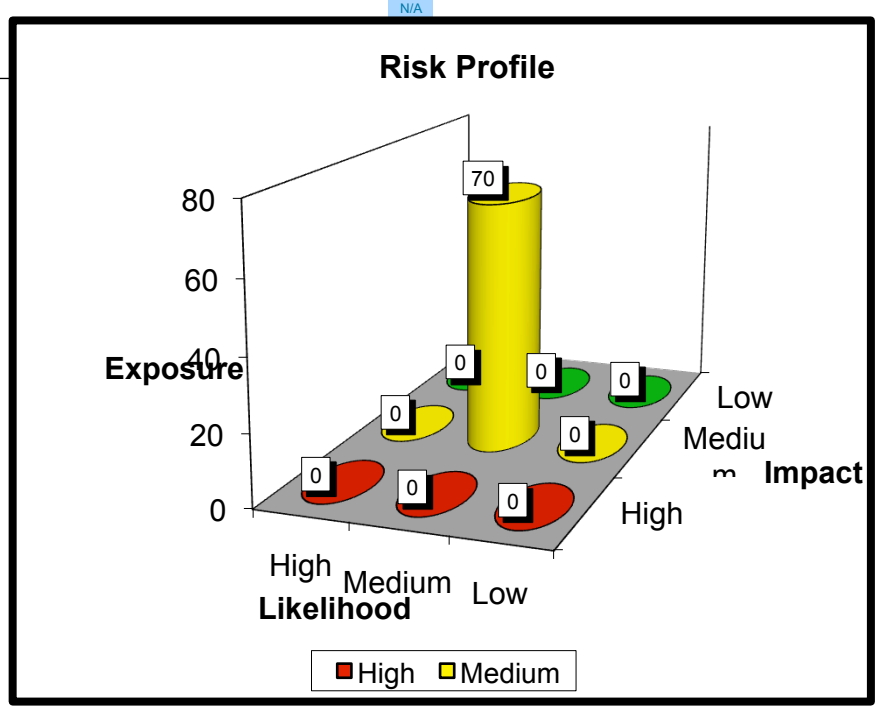
Giovanni Seppia, External Relations Manager

If you spot a shark…

- *Stay calm, as sudden movements may attract a shark*
- *Swim calmly and rhythmically back to land or boat*
- *Keep the shark in sight, particularly if you are swimming underwater. In most shark attacks, the victim did not see the shark. Sharks seem to shy away from people who look directly at them*
- *If all else fails, try to look prepared to fight back*

Where did we start from...

6. Premises including external data centres (see also 11.6)								
6.1 Short term evacuation for external reasons (petrol tanker on fire outside; riot or demonstration in street)	Not selected	Not selected	Not selected	Not selected	Not selected	*Minimize likelihood*	Choose "good" neighbourhood	N/A
							enforce boundary restrictions	N/A
						Minimize impact	Business backup site	N/A
							homeworking	N/A
							key information offsite	N/A
						Transfer risk		N/A
						Insure	Purchase cover	N/A
						Reaction plan	Invoke emergency plan	N/A
							telephone cascade procedure	N/A
6.2 Short term problem with the buildings (Legionnaires disease; dead body found; major break-in)	Not selected	Not selected	Not selected	Not selected	Not selected	*Minimize likelihood*	Good building maintenance & hygiene	N/A
						Minimize impact	Business backup site	N/A
							homeworking	N/A
							key information offsite	N/A
						Transfer risk		N/A
						Insure		
						Reaction plan		
6.3 Serious damage to the buildings some material/resources recoverable (Fire, hurricane; earthquake, flood, bomb)	Not selected	Not selected	Not selected	Not selected	Not selected	*Minimize likelihood*		
						Minimize impact		
						Transfer risk		
						Insure		
						Reaction plan		



The four dimensions of the registry business

- Process layer (core business, …)
- Technology (hardware, servers, software, applications, websites)
- People (HR)
- Logistics (buildings, sub contractors…)

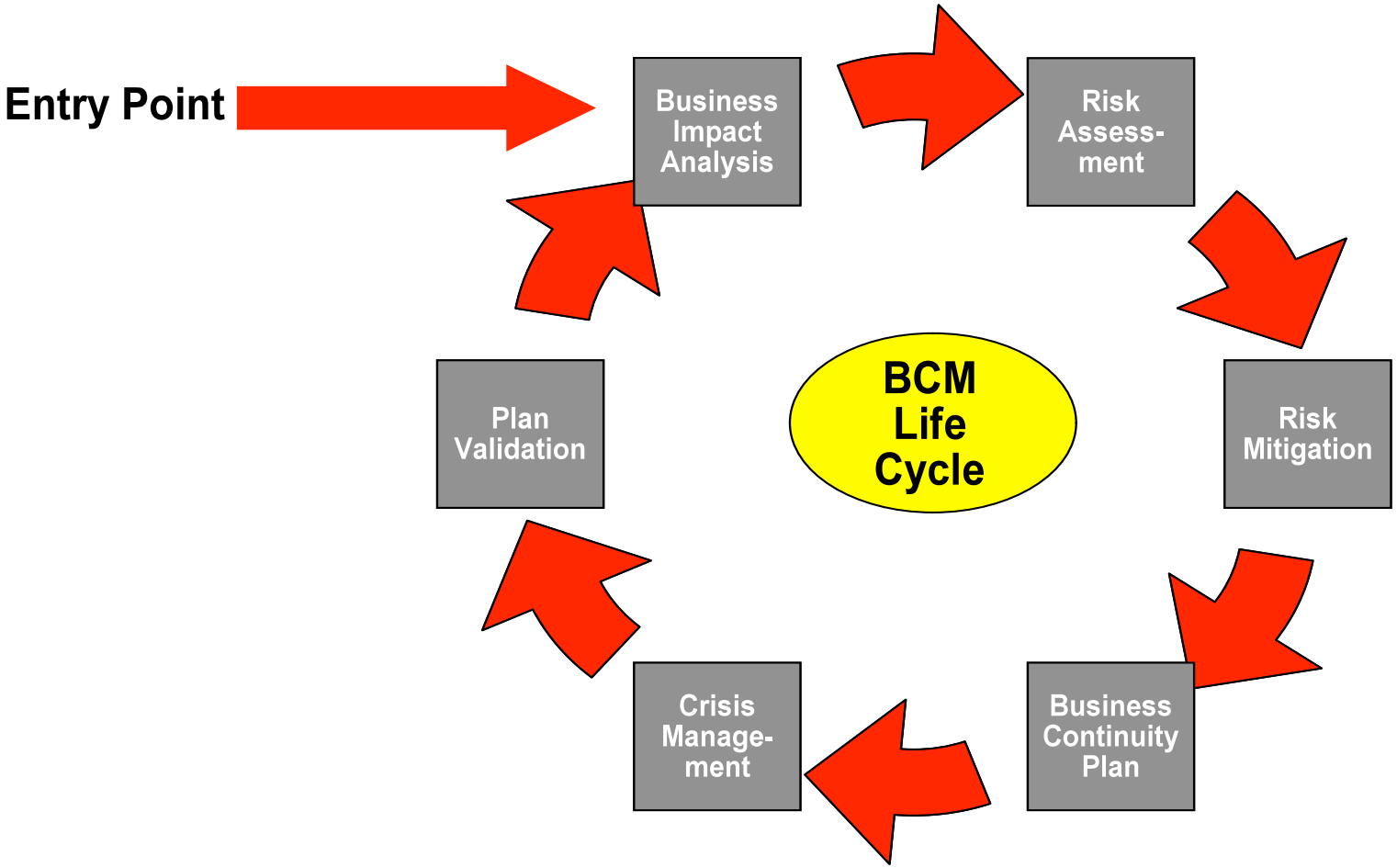
The outcome

- A set of documents:
  - The Business Continuity Plan, which includes the crisis management guidelines
  - The Disaster Recovery Plan
  - The Crisis Communication Plan
  - The Master BCP, which aims to provide a quick overview of the core elements of EURid BCP

- An approach shared by the entire company:
  - To see the BCP as a living process and therefore, to constantly improve the BCP framework
  - To test the effectiveness of the procedures as far as possible

- The assessment of our approach by an external company

The BCP approach



The EURid BCP approach

- To identify the EURid business processes and evaluate them through risk categories
- To assign to each of them risk assessment ratings
- To establish recovery time objectives in case of disaster/ calamity or in case that specific feature is unavailable
- To establish a list of those EURid processes to be considered critical according to the given ratings
- To cross-check the impact of different risk scenarios on the ten most critical processes
- To illustrate the procedures to be followed for each scenario in case the risk assessment has turn out to be ranked as “low”, “high” or “alarm” level

The BCP

- Shared with all staff members and regularly reviewed at management level
- Crisis management guidelines (crisis team, war room, emergency numbers,...)

Crisis Communication Plan

- Communications should be:
  - *Transparent*
  - *Correct*
  - *As timely as possible*
- Spoke person
- Target stakeholders
- Standard communication
- Communication channels

The test

- 25 April 2009: DRP-exercise (Disaster Recovery Plan) was executed to test EURid's business continuity capabilities
- Real scenario created
- Focused on our core Internet technical services
- Split into 3 phases. Registration system was moved to mirror site
- Successful: >10.000 transactions were successfully handled by the system
- Audited by an external party

Thank you!

giovanni.seppia@eurid.eu