



HOW STANDARDS AND CONFORMITY ASSESSMENT HELP TO MANAGE DISASTER-RELATED RISKS

27 April 2018

Questions

- ▶ 1. What challenges did your TC address with regards to disaster risk management when developing your standards. And what are the key standards?
- ▶ 2. In your opinion, how do these standards help prevent, reduce and manage disaster -related risks?
- ▶ 3. When developing your standards, how did you engage the various stakeholders, and specifically regulators, did you experience any challenges?
- ▶ 4. Did the regulators buy into the standards development process? What is your opinion in terms of level of confidence the regulators have in the standards and conformity assessment for asset management?
- ▶ 5. In your opinion, generally what the TC has achieved and what are the issues we still need to address with regards to disaster risk management and asset management ?

1. What challenges did your TC address with regards to disaster risk management when developing your standards. And what are the key standards?

Information security risks are most of the times not tangible and difficult to measure. The main challenge is to be able to establish risk criteria that are measurable, comparable and repeatable; that not only give a value to the risk to comply with a standard, but to give relevant information on determining the necessary controls, where to implement them and how strict those should be.

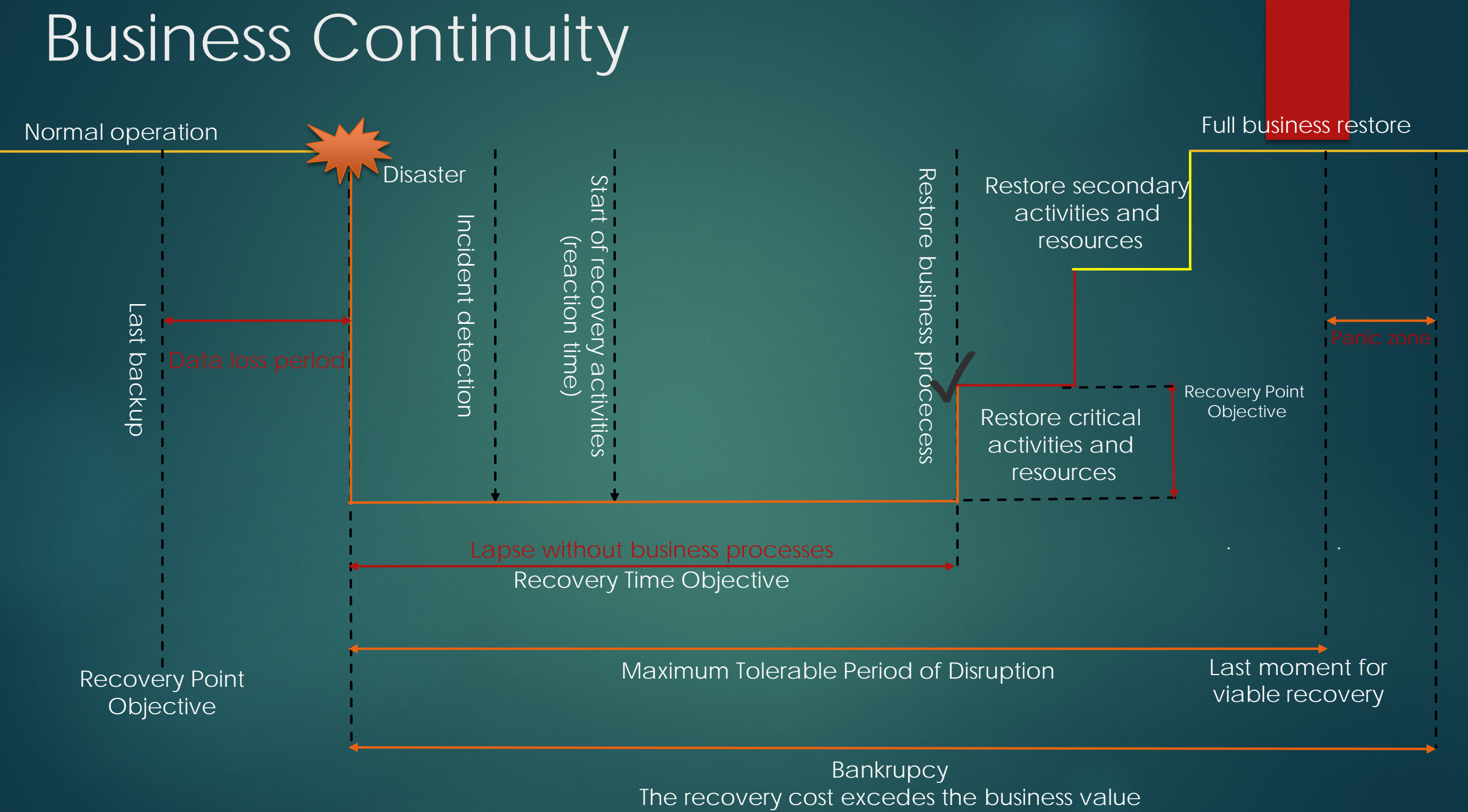
Key standards

- ▶ ISO/IEC 27001:2013 Information security Management System - Requirements
- ▶ ISO/IEC 27002:2013 Code of practice for information security controls
- ▶ ISO/IEC 27005:2011 Information security risk management
- ▶ ISO/IEC 27032:2012 Guidelines for cybersecurity

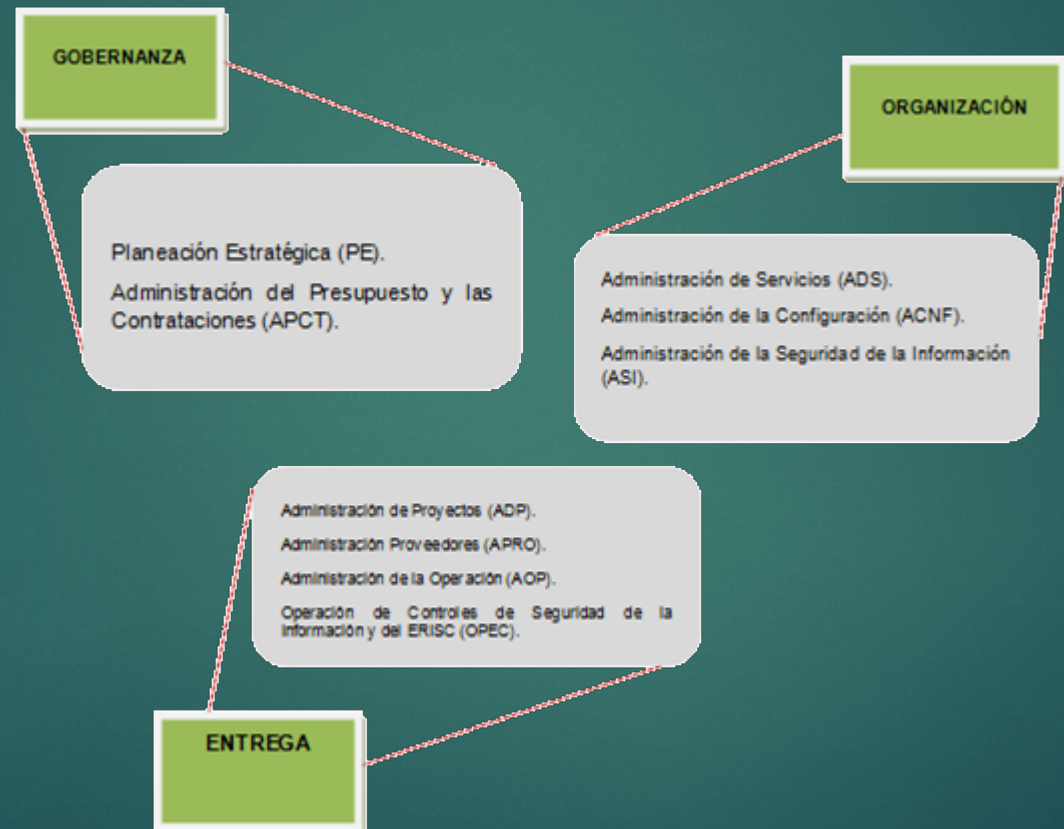
2. In your opinion, how do these standards help prevent, reduce and manage disaster - related risks?

- ▶ They establish a comprehensive framework for risk management, considering the different perspectives and interested parties. P.e Organization information, critical infrastructure, data protection, population rights and wellness
- ▶ Are adaptable to any organization, disregarding its size, sector or technological adoption
- ▶ Are compatible with other standards, such as ISO 22301, that can be established, implemented and maintained together

Business Continuity




3. When developing your standards, how did you engage the various stakeholders, and specifically regulators, did you experience any challenges?



Interested Parties





4. Did the regulators buy into the standards development process? What is your opinion in terms of level of confidence the regulators have in the standards and conformity assessment for asset management?

- ▶ Depends on the sector, a good example is Data Protection, where the authority has established a formal conformity assessment scheme and encourages organizations to comply and certify
- ▶ The National Cybersecurity Strategy is recommending the use of standards such as ISO/IEC 27001 and ISO 22301 to strengthen cybersecurity and protecting critical data and infrastructure from disasters

National Cybersecurity Strategy

Strategic objectives

Society and rights

Innovation and economy

Public institutions

Societal cybersecurity

Nacional cybersecurity

Transversal items

Cybersecurity culture

Capacities development

Coordination and colaboration


Reserch, development and innovation

Standards and technical criteria

Critical infrastructure

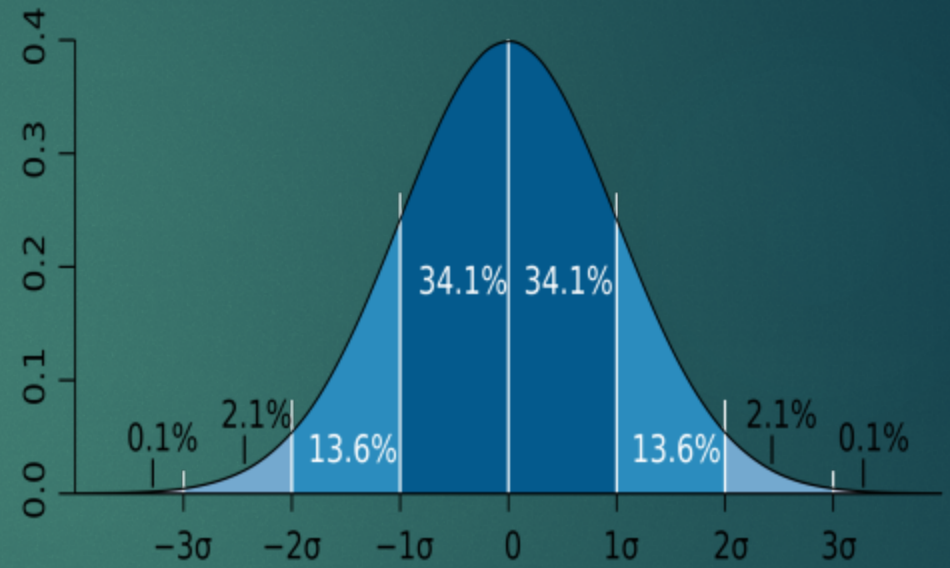
Legal framework and self-regulation

Measument and metrics

- 
- ▶ 5. In your opinion, generally what the TC has achieved and what are the issues we still need to address with regards to disaster risk management and asset management ?



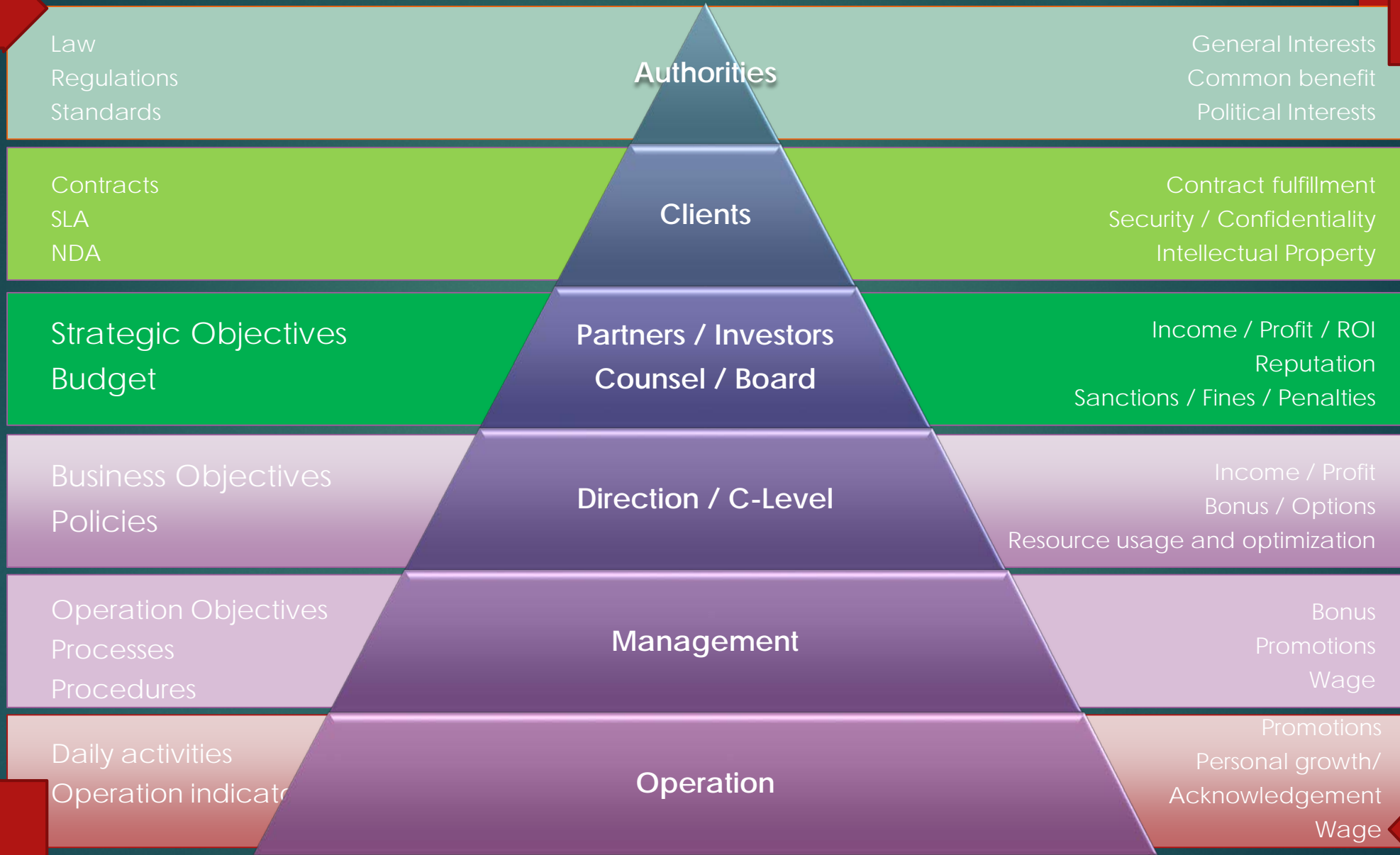
VS



Black SWAN events

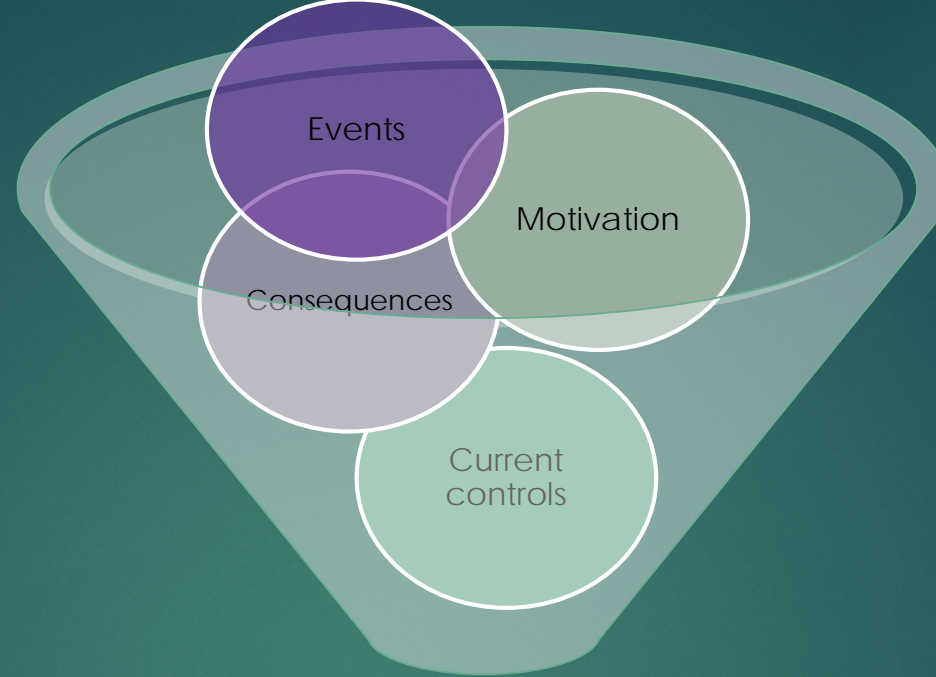
- ▶ The disproportionately high-impact, hard-to-predict role, and strange events that are outside the realm of normal expectations of history, science, finance, and technology.
- ▶ The non-computability of the probability of the rare consequential events using scientific methods (due to the very nature of the small probabilities).
- ▶ The psychological biases that make people individually and collectively blind to uncertainty and unconscious to the massive role of the bizarre event in historical affairs.
- ▶ The event is a surprise (for the observer).
- ▶ The event has a big impact.
- ▶ After your first record, the event is streamlined in retrospect, as if it might have been expected (for example, relevant data was available, but not posted).

Performance Indicators



Control objectives





Risk level

Necessary controls /
Update of current controls

Control type

Where is it needed?

How strict it should be

Measure risk

Risk come from business enablers, so taking risk is done to achieve an objective or to leverage on something that can make the organization to win something, but this winning comes with some possible **counterpart** that is the possibility that using those business enablers open the door for events that may have a **negative effect** in the organization.

We need to assess the **benefit of each business enabler** and whether the consequences of a negative effect **can be reduced** or to **prevent part or all the possibility** of the event to occur.

Thank you

Pablo Corona Fraga
Director General Adjunto
NYCE-SIGE

1204 5191 ext. 427

pcoronaf@nyce.org.mx



Twitter: @pcoronaf

