FACTOR Cascade Analysis

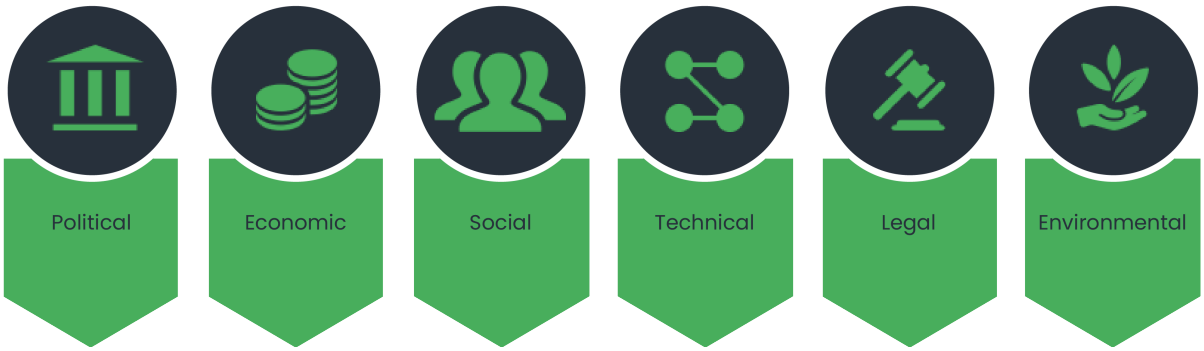
FACTOR Cascade Analysis; a shortcut examination of how external forces create threats and opportunities for the business and what this looks like in terms of risk.

Forces	What external forces are having impact?
Attributes	What are the characteristics of these forces? (size, scale & significance)
Cascade	What is the knock-on effect upon the organisation?
Threats	What are the emerging or immediate threats?
Opportunities	What are the emerging or immediate opportunities?
Risk	What is the risk to the business? (likelihood and impact)

Below are some guidance points when carrying out a cascade analysis.

F - Forces

Use PESTLE. PESTLE features in 'The Threat Horizon' - ISF's annual report which looks at the changing external landscape of information security risk. PESTLE is probably the most recognised tool for looking at external forces.



A - Attributes

Consider size, scale and significance

When looking at the *attributes* of external forces, it's important to identify the scale and escalating nature of the force.

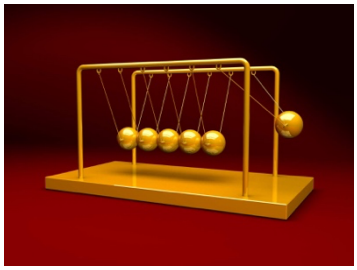
Is this a temporary event or is it something that has been building over time?

How disruptive is the external force to the Organisation and why is it happening?

Does the external force represent an adaptive change or a permanent shift? Can the Organisation adapt easily, or must it make wholesale changes, in order to respond?

Cascade

Cascade is where we consider which parts of the business are most impacted by changes in the external environment



External forces may be having a minimal or possibly seismic impact, on different parts of the operation.

Because information security is attached to every single part of the Organisation, security risks may need to be addressed across a wide range of different target environments.

It is important to understand where these external forces may be impacting the organisation and the knock-on effect this may have on information security.

T - Threats

Identifying threats can be categorised as those which are known vs unknown.

They may also be enterprise-wide threats created by a change in the external environment (E.g. a technological change) or, be internally driven (E.g. a weakness in existing infrastructure).

Threats to information security normally come in the form of:

Adversarial (e.g., hackers, nation states and insiders)
Accidental (e.g., malpractice and negligence)
Environmental (e.g., natural disasters).

In the information security domain, typical threats can be adversarial (e.g., hackers, nation states and insiders) accidental (e.g., malpractice and negligence) and environmental (e.g., natural disasters).

However, it's important to consider that threats to business continuity, are normally what dictate how information security risk is approached and managed.

O - Opportunities

Opportunities, normally appear as new ways of growing the business, increasing profitability or improving operational effectiveness

While the words risk and opportunity don't automatically sit hand-in-hand, the role of risk management isn't just to minimise the impact of threats but to also help the organisation realise opportunities

It could be opportunity cost (the cost in monetary terms of chasing an opportunity). Or, weighing up the change cost (how changing from the current path, or moving to a new option, might cost the business more (or less) in the long run

In either situation, the role of risk might be to help support the business (C-Suite) make the decision to go ahead with the opportunity

R – Risks

New risks must be benchmarked against the risk appetite of the organisation

Risks that present a likely impact need to be clearly identified, and assessed, with the risk appetite of the organisation in mind

Understanding the risk posture (ranging from risk seeking to risk averse) normally determined at the governing body or executive management level or a business unit level

Identifying the types and the levels of risk and to define, the maximum level of risk or harm that the organisation is prepared to accept (or can tolerate) in a given situation (risk tolerance).