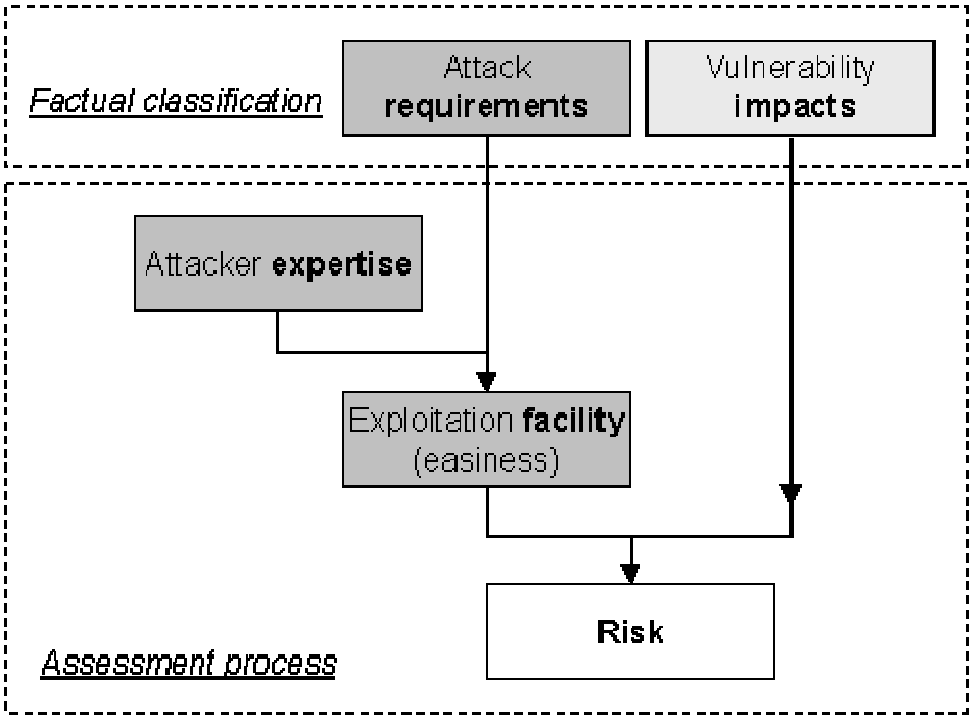
➢ Exploitation facility and risk (for an advisory)

The Cert-IST, according to the standard defined by the EISPP project (www.cert-ist.com/eispp) rates each published advisory to indicate to the reader the risk associated for a given information system. This evaluation relies on several parameters which combined lead to a single parameter named "**Risk**". The picture below shows a view of that process.



The **Risk Level** indicates to the reader how important the vulnerability is, and how urgently appropriate measures must be taken to counter the threat. The table below lists the Cert-IST recommendations on how to react depending on the risk level.

Risk	Recommendation
Very high	Act immediately on all systems
High	Act immediately on front-end systems and servers
Medium	Action can be delayed, but a security maintenance operation must be scheduled now
Low	Action can be delayed until the next scheduled maintenance operation

The tables below describe the method used for:

- combining the **attack Requirement** with the **Attack Expertise** to obtain the attack **Exploitation facility**.
- And combining this **Exploitation facility** with the vulnerability **Impact** to obtain the **Risk level**

	Requirement			
Expertise	Remote no account standard service	Remote no account exotic service	Remote with account	Physical access
Beginner	Trivial	Easy	Medium	Difficult
Skilled	Easy	Medium	Difficult	Very difficult
Expert	Difficult	Difficult	Very difficult	Very difficult

	Impact severity			
Exploitation facility	Take control	Get limited access Gain limited privilege	DoS Integrity impact Confidentiality impact	Disrupt service Leverage Hiding
Trivial	Very high	High	High	Medium
Easy	Very high	High	High	Medium
Medium	Very high	High	Medium	Medium
Difficult	High	Medium	Medium	Low
Very difficult	High	Medium	Low	Low