



Description

Study of the organization

- purpose, business, missions, values, strategies, structure

Asset classification

- Primary assets: business process & activities, information
- Supporting assets: hardware, software, network, personnel, site, structure

Constraints

- Organization -> political, cultural, personnel, strategic, territorial, economical, financial, structural, functional, timing, methodical etc.
- Scope -> pre-existing processes, technical, financial, environmental constraints, time, methodical, organizational etc.
- Risk modification -> time, financial, technical, operational, cultural, ethical, environmental, legal, ease of use, personnel, existing controls etc.

References

- <http://www.iso27001security.com/html/27005.html>
- ISO/IEC 27005:2011, Information technology – Security techniques – Information security risk management

Legend

- Output (Green shape)
- Process (Blue shape)
- Reference (Link) (Blue circle)
- Comment (Blue line)
- Decision (Blue diamond)
- Sub-process (Yellow shape)

Acronyms

- BCP: Business Continuity Plan
- C.I.A: Confidentiality, Integrity & Availability
- IEC: International Electrotechnical Commission
- InfoSec: Information Security
- IRP: Incident Response Plan
- ISMS: Information Security Management System
- ISO: International Organization for Standardization
- ISRM: Information Security Risk Management
- PDCA: Plan-Do-Check-Act
- RM: Risk Management
- RPM: Risk Management Plan
- RTP: Risk Treatment Plan



