8. Operations

- Establish criteria for processes
- Implement control of processes according to criteria
- Ensure documented information available to verify processes carried out as planned
- Control planned changes and review consequences of unintended changes
- Mitigate adverse effects of unintended changes
- Ensure externally provided processes, products, or services are controlled.

8.2 Information Security Risk Assessment

Regularly assess information security risks

Identify potential threats and vulnerabilities

Evaluate likelihood and impact of each risk

Take into account legal, regulatory and contractual requirements

Consider objectives and assets needing protection

Document and retain results of risk assessments

Include identified risks, likelihood and impact, and controls implemented

Track effectiveness of risk management activities

Inform decisions about future investments in security controls

8.3 Information Security Risk Treatment Plan

Risk Treatment Plan has to be implemented and documented

- **Which** controls to implement
- **Who** is responsible for them
- **What** are the deadlines
- **Which** resources are required

Example of Risk Treatment Plan

Control to be implemented	Risk reference	Responsible person	Deadline	Resources	Results
Install disk encryption on all laptops to protect data	Risk 46: data on lost or stolen laptops can be compromised	System administrator	16 April 2018	-2 man/days -bitlocker	Implemented
Install smart card physical control for data center	Risk 54: data center can be accessed by anyone	Facility manager	03 May 2018	Finances for control	Progress