Risk management Roadmap

Risk management (center)

Continuous monitoring

- Involve relevant risk, process and system owners
- Compare changes in residual risk to risk appetite
- Determine impact on residual risk
- Track external changes
- Track internal changes
- Monitor environmental variables
- Involve relevant risk, process and system owners
- Compare changes in residual risk to risk appetite
- Determine impact on residual risk
- Assess effectiveness of controls
- Evaluate performance of controls
- Track implementation of controls
- Evaluate risk mitigation

Risk treatment

- Implement controls
- Model the effect of controls
- Identify possible controls
- Identify limitations of risk treatment
- Model implementation of risk treatment
- Weigh risk assessment against risk appetite
- Risk avoidance
- Risk sharing
- Risk transfer
- Risk modification
- Recover
- Respond
- Detect
- Protect
- Risk mitigation
- Risicoacceptatie
- Risk acceptance
- Follow up on risk acceptance

Risk assessment

- Risk determination
- Impact determination
- Risk analysis
- Data collection
- Determine risk profiles
- Rank risk profiles
- Assess validity and reliability of risk assessment
- Follow agreed upon reporting mechanisms
- Assess impact on confidentiality
- Assess impact on availability
- Assess impact on integrity
- Quantify risk
- Qualify risk
- Identify interests to be protected
- Identify threats
- Identify resilience

Governance and preconditions

- Identify external factors
- Identify organizational structure
- Identify organizational security culture
- Identify alternative (organizational) strategies
- Identify security principles and risk management norms
- Context determination
- Align with organizational objectives, BCM and organizational priorities
- Integrate with enterprise risk management
- Organizational integration
- Identify security requirements
- Identify requirements defined by organizational policies, missions and business functions
- Identify requirements defined by laws, directives, regulations and standards
- Compliance identification
- Strategic leadership engagement
- Request direction and coordination from strategic leadership
- Establish risk appetite
- Secure mandate from strategic leadership
- Scope determination
- Develop portfolio overview
- Prioritize portfolio by organizational interests
- Prepare for risk assessment
- Governance formalization
- Identify roles and responsibilities
- Request approval of relevant risk, process and system owners
- Establish logging and reporting agreements
- Request approval on description of risk assessment scope
- Asign roles within risk assessment