Risk management

P. Jacques Houngbo
AIS 2013Technical Workshops
Lusaka, Zambia , June 2013

AfricaCERT
United in promoting cyber security in Africa

References

- This content is borrowed and adapted from a model created by University of Virginia
- http://its.virginia.edu/security/riskmanagement/

Contents

- Introduction: module objectives
- Raison d'être of risk management
- Terminology
- Process overview
  - Mission Impact Analysis
  - Risk Assessment
  - Mission Continuity Planning
  - Evaluation and Reassessment
- Conclusion

Contents

- Introduction: module objectives
- Raison d'être of risk management
- Terminology
- Process overview
  - Mission Impact Analysis
  - Risk Assessment
  - Mission Continuity Planning
  - Evaluation and Reassessment
- Conclusion

Introduction

- Objectives of the module :
  - Familiarize with the concept of risk management and its terminology
  - Discuss views on the rationale of risk management
  - Practice (express) from risk assessment up to business continuity plan
  - Focus on :
    - Practicality
    - Scalability

Contents

- Introduction: module objectives
- Raison d'être of risk management
- Terminology
- Process overview
  - Mission Impact Analysis
  - Risk Assessment
  - Mission Continuity Planning
  - Evaluation and Reassessment
- Conclusion

Raison d'être of risk management

- Business relies on the availability and reliability of IT assets
- Total failure or partial failure will compromise seriously and adversely affects the business
- IT Risk Management is a form of protection that the business can’t afford not to have
- Risk management is an exercise that creates (generates) consensus

Contents

- Introduction: module objectives
- Raison d'être of risk management
- Terminology
- Process overview
  - Mission Impact Analysis
  - Risk Assessment
  - Mission Continuity Planning
  - Evaluation and Reassessment
- Conclusion

Terminology

- Risk:
  - (Exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance; [Oxford English Dictionary]
  - Effect of uncertainty on objectives; [ISO 31000 (2009)]
- Risk Management:
  - identification, assessment, and prioritization of risks
  - followed by application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events

Risk Management (Simply Put): Determines what your risks are and then decide on a course of action to deal with those risks.

Contents

- Introduction: module objectives
- Raison d'être of risk management
- Terminology
- Process overview
  - Mission Impact Analysis
  - Risk Assessment
  - Mission Continuity Planning
  - Evaluation and Reassessment
- Conclusion

Process overview

- IT Mission Impact Analysis :
  - Identification of critical assets
- IT Risk Assessment :
  - Study of threats and vulnerabilities, effectiveness of present security mechanisms
  - Creation (or update) of security plan for mitigating or accepting the identified risks
- IT Mission Continuity Planning :
  - Creation (or update) a response plan to use in the event that critical IT assets are lost, unavailable, corrupted or disclosed
- Evaluation and Reassessment :

Contents

- Introduction: module objectives
- Raison d'être of risk management
- Terminology
- Process overview
  - Mission Impact Analysis
  - Risk Assessment
  - Mission Continuity Planning
  - Evaluation and Reassessment
- Conclusion

Mission Impact Analysis

- Identification of IT assets
- Identification of critical IT assets

- Critical IT Asset:
  - IT Assets that when disclosed, modified, destroyed, or misused will cause harmful consequences to the business or will provide an undesired and unintended benefit to someone

- Risk management process - Step 1 - IT Mission Impact Analysis.docx

Contents

- Introduction: module objectives
- Raison d'être of risk management
- Terminology
- Process overview
  - Mission Impact Analysis
  - Risk Assessment
  - Mission Continuity Planning
  - Evaluation and Reassessment
- Conclusion

Risk Assessment

- Assess departmental security practices
- Threat, attack and vulnerability scenarios
- Security plan development

- Risk management process - Step 2 - IT Risk Assessment.docx

Contents

- Introduction: module objectives
- Raison d'être of risk management
- Terminology
- Process overview
  - Mission Impact Analysis
  - Risk Assessment
  - Mission Continuity Planning
  - Evaluation and Reassessment
- Conclusion

Mission Continuity Planning

- What to do in the event that the mitigation responses from Step 2 prove to be insufficient or if an unmitigated risk becomes a reality?

- Risk management process - Step 3 - IT Mission Continuity Planning.docx

Contents

- Introduction: module objectives
- Raison d'être of risk management
- Terminology
- Process overview
  - Mission Impact Analysis
  - Risk Assessment
  - Mission Continuity Planning
  - Evaluation and Reassessment
- Conclusion

Evaluation and Reassessment

- IT changes rapidly, so do the risks it face
- Environment of the business is also evolving
- You may run Evaluation and Reassessment every two to three years

- Risk management process - Step 4 - Evaluation and Reassessment.docx

Contents

- Introduction: module objectives
- Raison d'être of risk management
- Terminology
- Process overview
  - Mission Impact Analysis
  - Risk Assessment
  - Mission Continuity Planning
  - Evaluation and Reassessment
- Conclusion

Conclusion (1/2)

- Some recommendations
  - The question is not if risks can turn to disaster, (probability to reality), the question is when
  - Preparation is vital, learn from militaries
  - The better you know your assets, the better you'll "manage" uncertainty
  - Risk Management is never a completed process
  - The final point is that IT must continue to be an enabler for the business

Conclusion (2/2)

“If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology”- Bruce Schneier

http://think.securityfirst.web.id/?page_id=12

P. Jacques Houngbo
jacques.houngbo@africacert.org

AfricaCERT
United in promoting cyber security in Africa