IS4231
Information Security Management

Course Review & Final Exam Briefing

AY 2021/2022 Semester 1

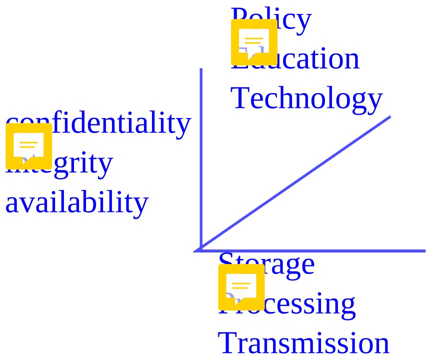
Lecturer: Dr. YANG Lu

Email: yanglu@comp.nus.edu.sg :: **Tel**: 6516 6791 :: **Office**: COM2-02-46

Course Review

L1 Introduction

- What is information security
- Communities of Interest
- Specialized Areas of Security
- CNSS Security Model
- The CIA Triad and extension
- Different Management Roles
  - Information, interpersonal, decisional role
- Six Ps:
  - Planning, Policy, Programs, Protection, People, Project Management



need to achieve balance between protection and availability

L2 Compliance

- Professional Code of Ethics
- Law
  - Local law
    - Cybersecurity Act
    - Computer Misuse Act
    - PDPA
  - International law
    - GDPR 2018
    - CCPA 2018
- Industry regulation
  - MAS TRM Guidelines

Links to the Cybersecurity Code of Practices

minimum protection policies that CIIO must implement for their CII

Criteria

Difference between GDPR, CCPA & PDPA

OT cybersecurity masterplan 2019
- focus on OT

L3 Governance and Planning for Security

- Planning levels
  - Strategic, tactical, operational
- Planning approaches:
  - Top-down vs. bottom-up
  - Pros and cons
- What is Governance
  - Benefits
  - Responsibilities
- SesSDLC
  - Cycles

Using the ISO 270014
Standard for governance

L4 InfoSec Policies

Basic rules of policy
1. Never conflict with law
2. Must be able to stand up in court if challenged
3. Must be properly supported and administered

- What is policy and why policy?
- Policy, Standards, and Practices
- Successful Policy Characteristics
- Types of InfoSec policies
  - Enterprise Information Security Program Policy (EISP)
  - Issue-Specific Security Policy (ISSP)
  - System-Specific Security Policy (SysSPs)
- Guidelines for effective policy development and implementation

L5 InfoSec Program

- Placing InfoSec Within an Organization
  - Pros and cons in each approach
- Staffing the Security Function
  - Roles
  - Ratio
- Components of a security program
  - NIST model
  - ISO/IEC 27000s model

L6 Security Management Practices

Security Employment Practices

- Before hiring
  - Background Checks
- During employment
  - Separation of duties
  - Two-man control
  - Need to know and least privilege
  - Job rotation/task rotation
  - Mandatory vacation
- Termination Issues
  - Non-to-compete
  - Garden leave
  - No-Disclosure Agreement

NUS issuing electronic degree scrolls through OpenCerts platform - based on BlockChain technology

Difference between separation of duties and 2 man control

Difference between need to know and least privilege

L6 Security Management Practices (cont.)

- Performance measurement
  - Benefits
  - Factors to be considered when devising measures
  - Types
    - Implementation
    - Effectiveness/efficiency of delivery
    - Impact
- What is a good performance measure?

Examples:

L7 Security Management Models

- Security Management Models
  - ISO/IEC 27000 series
  - CSA Star program
  - NIST security models
  - COBIT
  - PCI DSS
  - ISF the Standards
  - CIS Standards
- Low Level Security Models
  - Evaluation models
    - Common Criteria

All iso

CSA cybersecurity labelling scheme

ISO/IEC 27k5 Risk management

L8 Risk Assessment

- Risk Identification
  - Identification and prioritization of information assets
    - Assess value

      Weighted table
  - Threat Modeling
    - Threat identification
    - Threat Assessment and prioritization
      - □ Vulnerability assessment
  - The TVA worksheet
- Risk Assessment
  - The risk formula
  - Ranked vulnerability risk worksheet
- Risk Appetite

L9 Risk Treatment

- Risk Control
  - Five control strategies
    - Defense, transference, mitigation, acceptance, termination
  - Feasibility analysis
    - Economic: cost-benefit analysis
      - □ SLE, ALE, CBA
    - Other Feasibility Measures
      - □ Organizational feasibility
      - □ Operational (or behavioral feasibility)
      - □ Technical feasibility
      - □ Political feasibility
  - Alternatives to feasibility analysis
  - Risk Scenario documentation
  - Qualitative and hybrid measures

ISO27005 InfoSec Risk management
ISO 31000 Risk management

L10 Planning for Contingencies

- What is Contingency Planning
- Business Impact Analysis
  - Key recovery measures
    - MTD, RTO, RPO, WRT
- Incident Response Plan
  - Detection, Reaction, Recovery
- Disaster Recovery Plan
- Business Continuity Plan
  - Exclusive-use options
  - Shared-use options
- Crisis Management Plan
- Testing contingency Plan

Incident Contingency Planning

AWS cloud as continuity strategies

Tutorials

- T1 – Introduction to InfoSec
- T2 – InfoSec Compliance
- T3 – Cyber Breach at Target
- T4 – Global Data Protection Compliance
- T5 – Mandated InfoSec Program at Zoom
- T6 – InfoSec Policies and Governance at NUS
- T7 – Singapore HIV Data Breach
- T8 – PCI DSS and Common Criteria
- T9 – Risk Management

Others:

- Guest Talk:
  - Basic idea of essential points
- Reading materials
  - Only for what we've discussed in class, will be tested.
  - Otherwise, for your own learning purposes.

Peer Review

- LumiNUS-Survey: Peer Review
  - Optional
  - Only if you have issues regarding team member contribution
  - Feedback you provided:
    - Be as specific as possible
  - Get it done by:
    - 1159pm, 17 Nov (Wed), 2021

CA marks and feedbacks release

- By this week:
  - Tutorial attendance marks
  - Tutorial participation
  - Tutorial discussion leading
- By next week
  - Project report
    - Grade – LumiNUS Gradebook
    - Feedback – via Email

Final Exam Briefing

Final Exam

- Percentage: 50%
- Channel:
  - LumiNUS-Quiz
    - Can be resumed multiple times
    - Can turn back to previous questions
  - Time:
    - 5pm – 7pm, 29 Nov 2021, Mon
  - Duration:
    - 2h
  - Coverage:
    - All lecture, tutorial content and guest talk are examinable

Final Exam (cont.)

- Exam format
  - Open book

- Question format
  - MCQ (10%):
    - 20 questions
    - 0.5 marks for each question
  - MRQ (5%):
    - 5 questions
    - 1 mark for each question
    - No partial mark
  - TOF (5%):
    - 5 questions
    - 1 mark for each question
    - No partial mark given
      - True questions: no need explanation
      - False question: need explanation
  - Structured questions (30%)

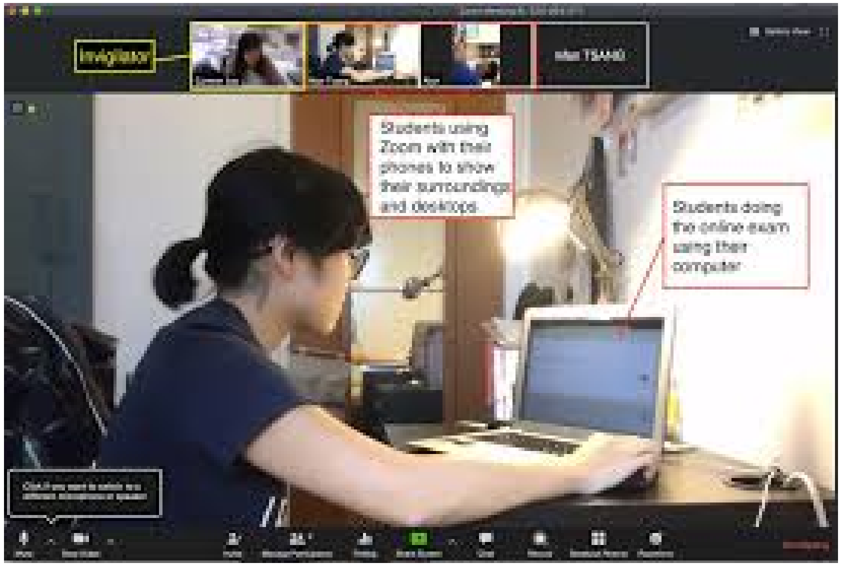
Final Exam (cont.)

- Communication channel:
  - Communication with examiner/invigilator
    - MS Teams
    - Use emails if MS Teams is down
  - Public announcement:
    - MS Team chat
    - Zoom audio
- Proctoring

1. Only one display is allowed, no multiple displays
2. Zoom proctoring
3. Screen recording
4. Should NOT use Internet search or have any communication with others during the exam.
5. Lecture/tutorial notes/reading materials could be accessed on computer.

Final Exam (cont.)

- Proctoring
  1. Only one display is allowed, no multiple displays.
  2. Zoom proctoring:
     - Second device (e.g., smartphone)



Students using Zoom with their phones to show their surroundings and desktops

Students doing the online exam using their computer

Final Exam (cont.)

- Proctoring

  3. Screen recording:

     - The recorded video should be uploaded **on Luminus Files-> Screen recording video submission folder** by **8pm**, 29 Nov 2021 (within 1h after the test ends)
     - Suggested tools:
       - □ Ffmpeg
       - □ VLC media player
       - □ QuickTime Player (Mac OS)
     - Computer space:
       - □ Gauge:
         - □ 2-hour exam will generate a video file of about 100 MB in size.
         - □ Might be larger and around 200MB using various tools.

Final Exam (cont.)

- Attention:
  - Pls double check and test your 2 devices (one for answering exam questions, one for zoom proctoring) and make sure that they are in good function.
  - This is your responsibility.

Final Exam (cont.)

- Contingency plan:

  1. LumiNUS-quiz

     - If LumiNUS- quiz is down for less than 30 mins:
       - □ Delayed accordingly.
     - If LumiNUS- quiz is down for more than 30 mins:
       - □ Will send you the encrypted PDF with exam question inside and the password
       - □ Answer the questions using Word (a template available in LumiNUS-Lecture Notes folder).
       - □ Covert the word file to pdf, name it use your student matric number, and submit the PDF file of your answers to a designated LumiNUS file folder :
         - □ exam answer submission folder

Final Exam (cont.)

- Contingency plan:

  2. Zoom

     - If zoom server is down during exam:
       - □ Continue without proctoring

  3. Second pc for proctoring failure

     - Inform the invigilator immediately over MS Teams private chat.
     - Convert to use PC's webcam for proctoring.

  4. PC failure

     - Inform the lecturer immediately over MS Teams private chat

  5. Screen recording failure

     - Inform the lecturer immediately over MS Teams private chat
     - Be careful, if you failed to successfully record the screen and upload the video, you might receive a warning from the school.

Good luck with the exam!