NIE
NATIONAL INSTITUTE OF EDUCATION
SINGAPORE

# Response to Cyber Security Threat

TRANSFORMING TEACHING
INSPIRING LEARNING

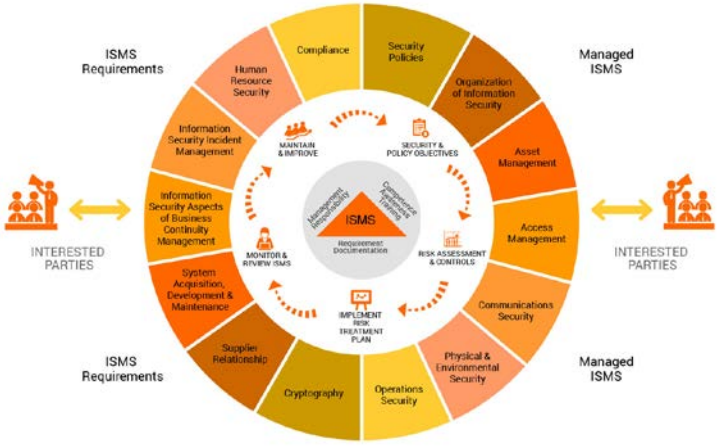
# NIE's Approach to Information Security

- Background – NTU / NIE is corporatized in April 2006 (Not requires to comply with IM8)

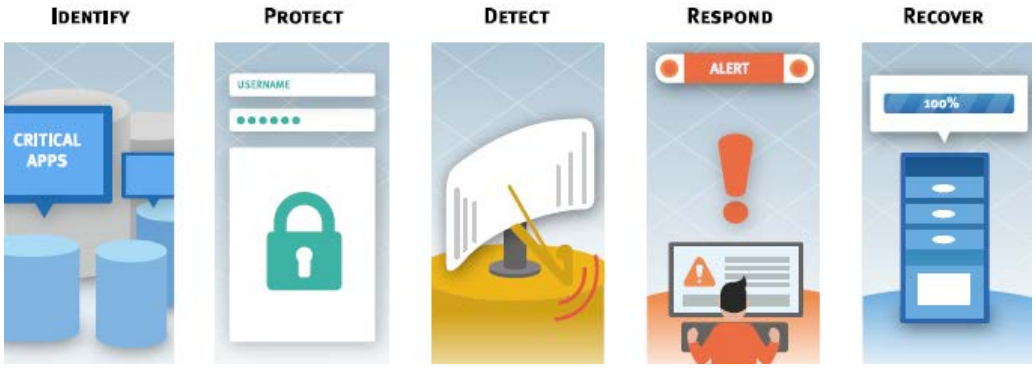
- Mission - To provide effective ICT resources, services and infrastructure that would enable NIE to be an Institute of Distinction
- Strategy – Risk-based approach to manage NIE cyber security

# Journey of NIE Information Security

- Getting buy-in from senior management
- Setting up information security team
  - Covers both ICT and non-ICT security risk
- Adoption of standard and framework
  - Implementation of process centric information security management
  - ISO 27001 as the standard for managing information security
  - Continuous improvement (PDCA) being core to the standard



# Response to Cyber Security Threat




- Identify
  - Understand the critical business function and possible business and IT risk
  - Review cyber security profile and incident regularly
- Protect
  - Patch management
  - Mitigation controls

# Response to Cyber Security Threat (cont)

- Detect
  - Manage security event and information holistically
  - Dedicate resources to response to cyber security incident
- Respond
  - Conduct incident response (cyber security) exercise on a periodic basis
  - Awareness and training
  - Collaborate with industry partners such as Cyber Security Agency, Singapore Police Force, cyber security experts (Incident response and forensics), etc
- Recover
  - Business continuity exercise
  - Engage legal and cyber security insurance services


ANY
QUESTIONS
?