# NON-TECHNOLOGICAL AND ETHICAL ASPECTS IN CYBERSECURITY AUDIT

Yullyan, SE,MAk,CA,CPA,CIA

# YULLYAN, SE, MAK, CA, CPA, CIA

## EDUCATION

- INDONESIA UNIVERSITY, ACCOUNTING, MASTER
- BRAWIJAYA UNIVERSITY, ACCOUNTING, BACHELOR
- STAN, ACCOUNTING, DIPLOMA

## WORK EXPERIENCE

- MERATUS LINE, INTERNAL AUDIT MANAGER, 2019 – NOW
  - LEAD DIGITAL AND AGILE TRANSFORMATION OF INTERNAL AUDIT
  - ADVISOR OF CYBERSECURITY INITIATIVES, ERP TRANSFORMATION
- BP INDONESIA, CONTROLLER, AUDIT LEAD, 2013-2019
  - SAP TRANSFORMATION, AUTOMATION, FINANCIAL CONTROLS
  - JV AUDIT, COMPLIANCE AUDIT, CONTROL REVIEW AND ENHANCEMENTS
- PREMIER OIL, TAX SECTION HEAD, 2012-2013
  - TAX COMPLIANCE MANAGEMENT
  - DISPUTE MANAGEMENT
- CNOOC, HEAD OF AUDIT, 2010-2012
  - RISK MANAGEMENT
  - JV AUDIT, COMPLIANCE AUDIT, IT AUDIT, CONTROL REVIEW AND ENHANCEMENTS
- BPK-RI, AUDIT SECTION HEAD, 1998-2010
  - LEAD GOVERNMENT FINANCIAL STATEMENT AUDIT
  - LEAD INVESTIGATIVE AUDITS

Cyber Security

Policies and Procedures

Technology
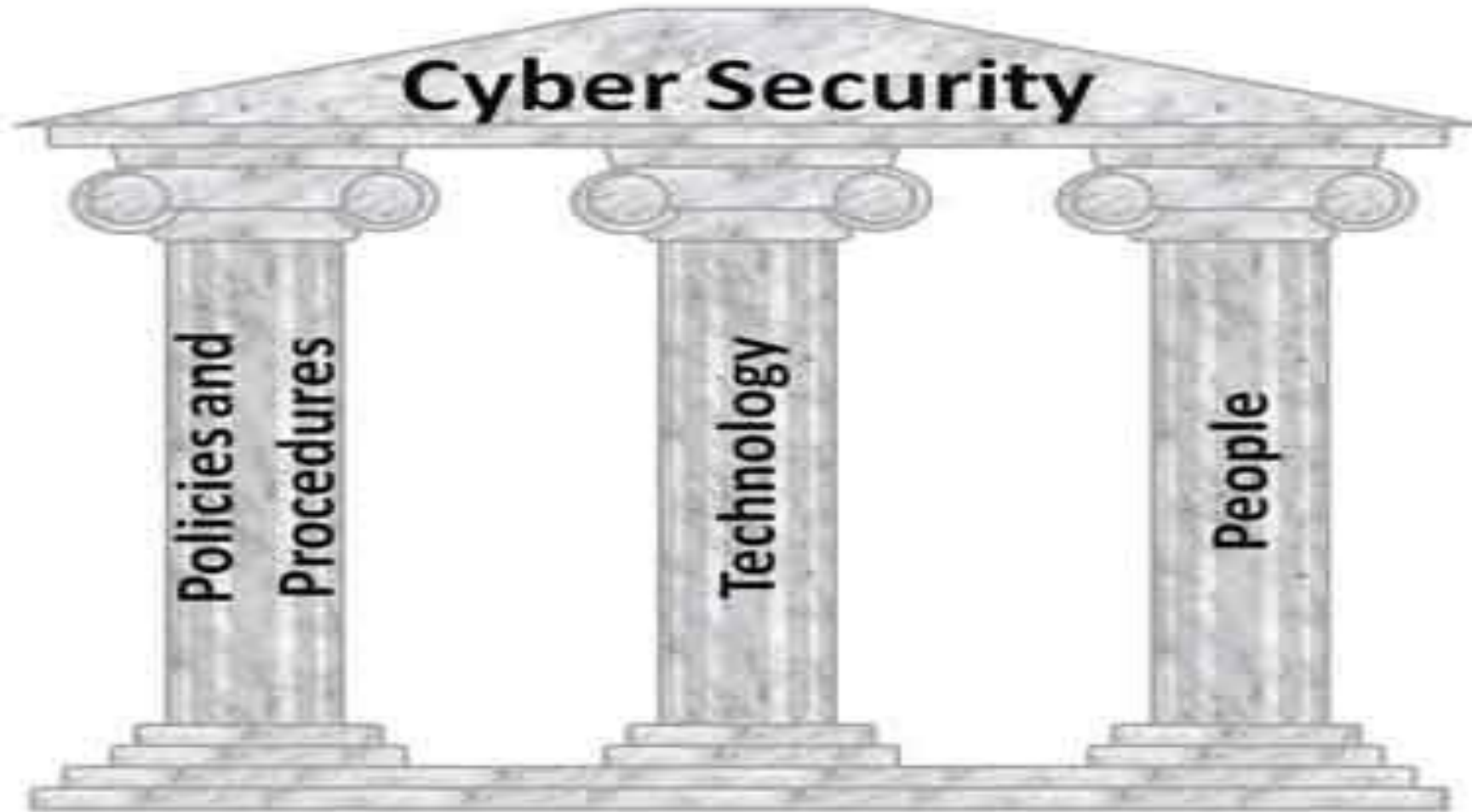
People

# WHAT AND HOW TO AUDIT A PEOPLE ASPECT

- Training and Awareness of cybersecurity
  - Review training and awareness program performance
  - Review the contents (phising, user access, malicious softwares, etc)
  - Review the competency test materials
  - Review the dashboards contents and updates (visibility of threats)
- Collaborate with IT for ethical phising attempts
- Observe the security behaviours in every audit engagement or in daily observations
- Review IT Security competencies
- Review system admin works

# WHAT AND HOW TO AUDIT A POLICY/PROC ASPECT

- Review policies and implementation of :
  - User access management (add, monitor, remove)→ GTAG 9 Identity and Access Management
  - Software asset management
  - BYOD
  - Cloud services
  - Change and Patch management
- Review the procedures and implementation of the above. Also review:
  - Integration of HR procedures with UAM, BYOD
- Review contract with cloud provider
- Review cloud provider security certification (SOC type 2 should available)
- Review the incident response and procedures

# ETHICAL CONSIDERATIONS

- Confidentiality of data regulated in different regulations (tax, financial services, health)
- Menkominfo Regulation 20/2016 : Personal Data Protection in Electronical System
- When to tell customer about the data breach incidents?
- Privacy and confidentiality issues when IT can see and tracking your devices, including BYOD→ GTAG 5 Managing and Audit Privacy Risks
- Licensing issue

# Thank You

# Bonus Slides

# Active Auditing

Traditional audits are often awash in wasted time, unnecessary conflict, and incorrect assumptions. Active auditing is a form of Agile auditing that was developed in a major utility company to eliminate, or at least substantially decrease, these kinds of wasteful activities.

## Lean and Agile Combined

- Lean : Toyota Production System-Change Making Methodology

- Agile : IT Project Management approach, an alternative to waterfall approach

## COMBINING LEAN AND AGILE TECHNIQUES

**PRINCIPLES FROM LEAN**
- » Waste is disrespectful
- » Visual management
- » Customer defines value
- » Standardized work
- » Respect for people

**PRINCIPLES FROM AGILE**
- » Iterative development
- » Time-boxing
- » Value-based prioritization
- » Collaboration
- » Empirical process control
- » Retrospectives

**ACTIVE AUDITING PRINCIPLES**
- » PILLAR ONE – Energetic collaboration
- » PILLAR TWO – Iterative audit execution
- » PILLAR THREE – Visual management
  - » Objectives-based risk assessment
  - » Experimentation
  - » Retrospectives

Ref : Coleman, Prescott, Active Auditing – A Practical Guide to Lean and Agile Auditing, 2019