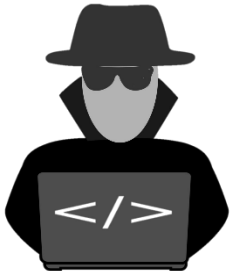# Enterprise Cybersecurity

From Strategy to Operating Model
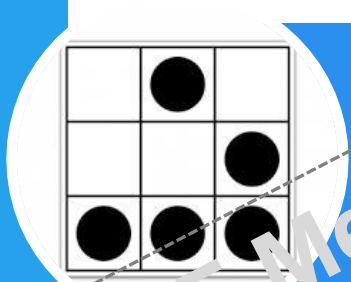
11th Meetup | 27 Feb 2020
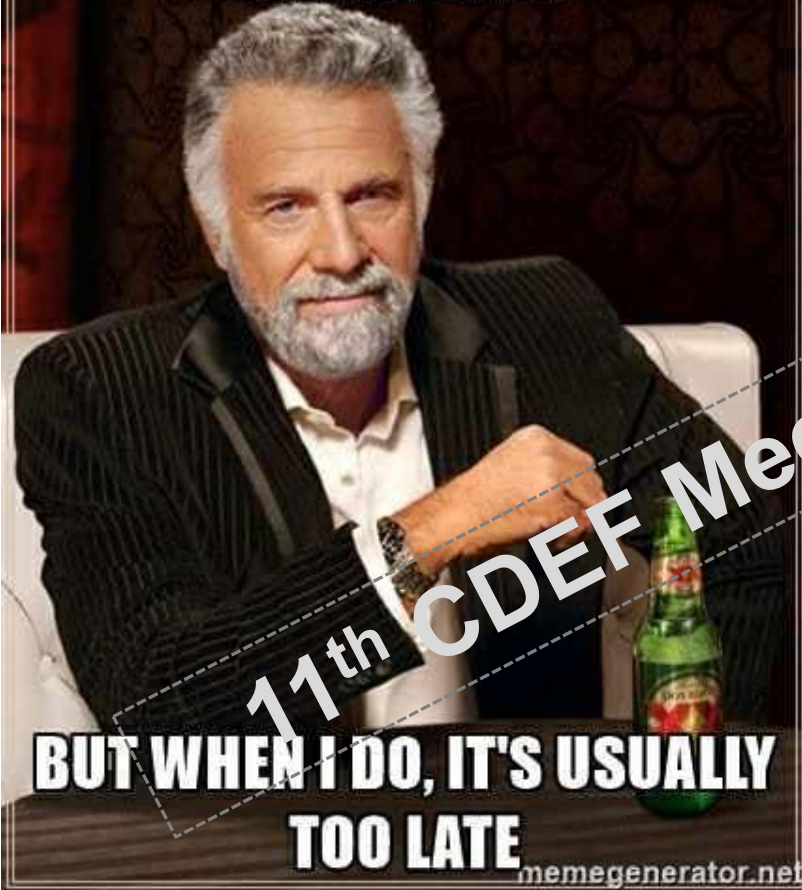
Eryk Budi Pratama

WHO AM I?

- Cyber Security & Community Enthusiast
- Cybersecurity & IT Advisory Consultant, Global Consulting Firm
- Experiences: CyberSec, IT GRC, IT Audit, IT Advisory
- Versatilist
- Knowledge Hunter
- Do some "magic"
- **https://medium.com/@proferyk**
- **https://www.slideshare.net/proferyk**

Let's Start

I DON'T ALWAYS THINK ABOUT CYBERSECURITY

BUT WHEN I DO, IT'S USUALLY TOO LATE

memegenerator.net

11th CDEF Meetup – 27 Feb 2020

Why we need strategy at first?

Source: https://archerint.com/what-is-cybersecurity/

Enrich and leverage your point of view are very important to develop
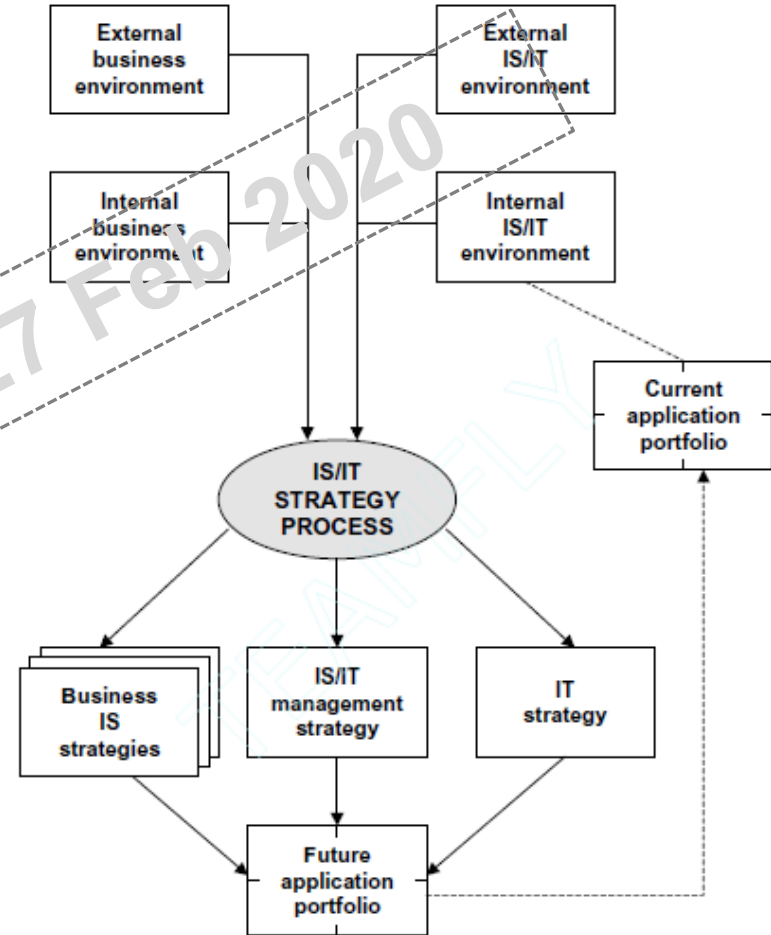# *cybersecurity strategy and operating model*

Theory when I was in college

Ward & Peppard Model, 2002

Strategic information system planning

Keywords:
- ❑ Business environment (external and internal)
- ❑ IS/IT environment (external and internal)
- ❑ Business IS strategies
- ❑ IT strategy and management
- ❑ Application portfolio (current and future)

Accumulation of my experiences

Local Projects	Regional Projects	Global Projects
• Financial Services • Maritime • Startup • Education	• Oil & Gas • Telco	• Financial Service

Related Personal Experiences

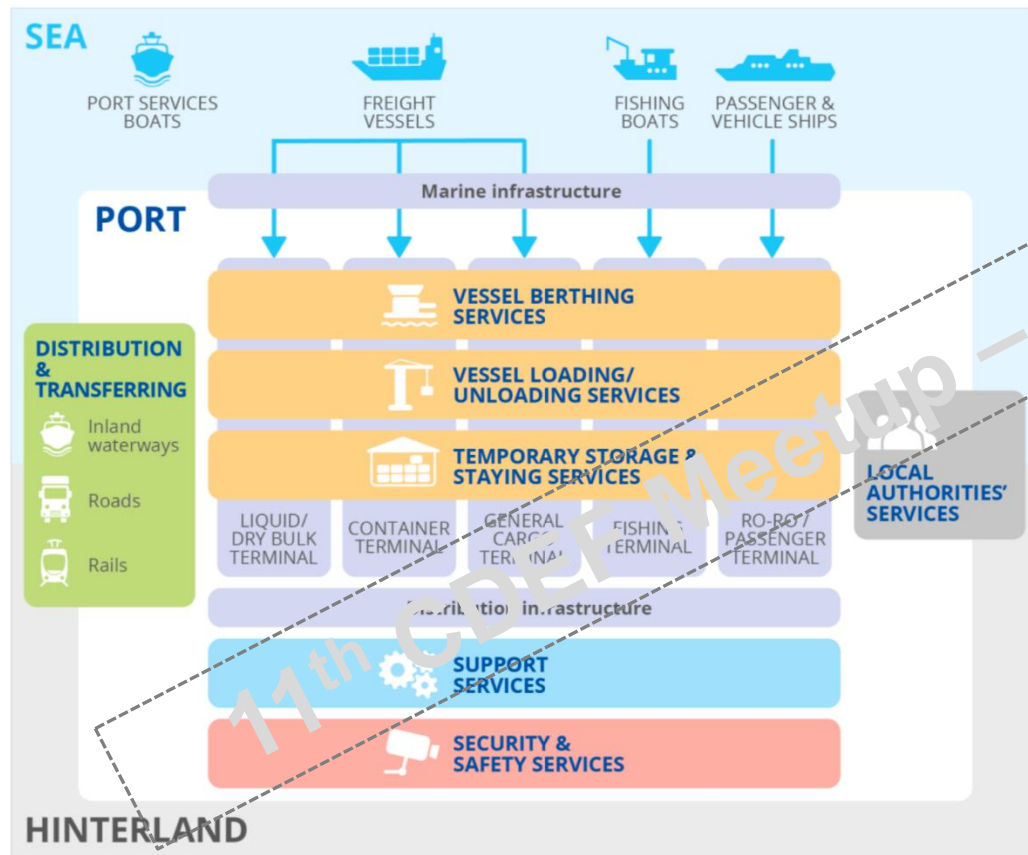| IT Strategic / Master Plan	Cybersecurity Transformation	IT Maturity Assessment
IT Audit	IT Governance, Risk, Compliance	Technical Assessment	Third Party Risk
Technology & Security Architecture	Business Case Development	others ☺

Understand the business is very important

What should we learn?
- ❑ Related regulation
- ❑ Services
- ❑ Key stakeholders
- ❑ Reference model of port systems
- ❑ Data and information flow
- ❑ Asset taxonomy (IT & OT) – Crown Jewels
- ❑ Threat taxonomy
- ❑ **BENCHMARK**

Source: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

Concept + Experience + Benchmark

Make it happen !!

Where is my cybersecurity budget?

Source: https://i.redd.it/ywjqwsmrftx31.jpg

Cyber Security Strategy Development

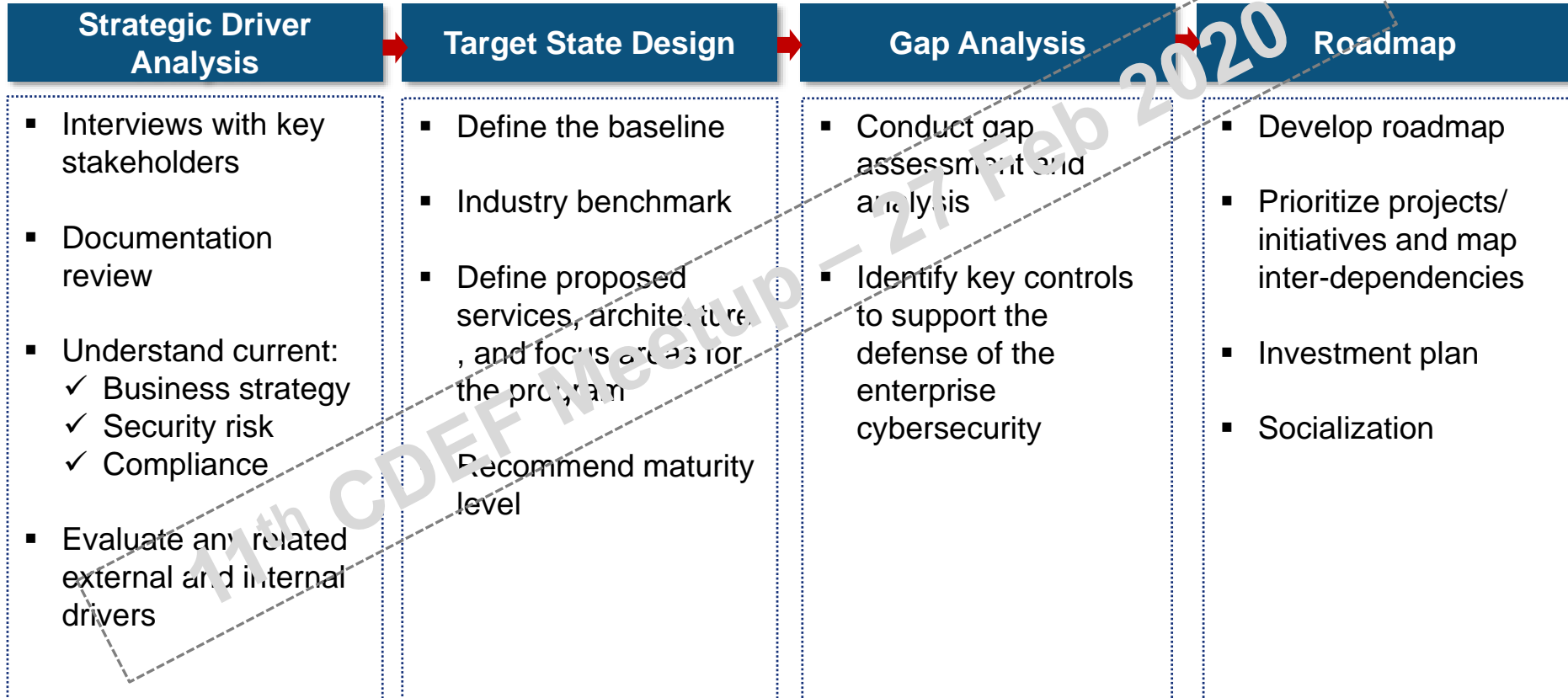# Common mistakes in cyber strategy development

Common mistakes based on my experience and other people deliverables

- **Lack of "context" (external and internal) understanding**

- **Limit perspective / point of view on cybersecurity only**

- **Lack of key stakeholder involvement**

- **Focus only on "gap assessment" and "maturity level" result**

- **More focus on TECHNOLOGY aspect**

upss ! ☺

Basic process

Strategic Driver Analysis	Target State Design	Gap Analysis	Roadmap

Strategic Driver Analysis
- Interviews with key stakeholders
- Documentation review
- Understand current:
  - ✓ Business strategy
  - ✓ Security risk
  - ✓ Compliance
- Evaluate any related external and internal drivers

Target State Design
- Define the baseline
- Industry benchmark
- Define proposed services, architecture, and focus areas for the program
- Recommend maturity level

Gap Analysis
- Conduct gap assessment and analysis
- Identify key controls to support the defense of the enterprise cybersecurity

Roadmap
- Develop roadmap
- Prioritize projects/ initiatives and map inter-dependencies
- Investment plan
- Socialization

What should considered as the input

Several recommended input based on my experience

- **External and internal context (e.g regulation, business trends)**
- **Current and future threats (OT & IT)**
- **Current and future risks (Threat Actors, Targets, Methods, Vulnerabilities)**
- **Stakeholder (business) expectations**
- **Audit finding**
- **Current IT Strategic Plan**
- **Enterprise Architecture (Security Architecture)**

Find the key problems is the best way to start !!

How we combine all insights

Activities we should consider

- Documentation review
- Interview
- Workshop / FGD
- Questionnaire
- Gap Assessment
- Maturity Assessment

Determine your:
- **Baseline**
- **Framework**
- **Standard**

What should considered as the input

Deliverables

- Cybersecurity strategy themes, goals, and initiatives
- Transformation journey / roadmap
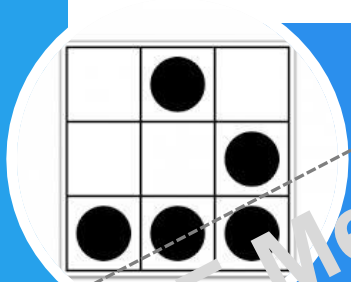- Program and Organization Structure
- Operating Model — **Next topic**
- Investment Plan / Budget

11th CDEF Meetup – 27 Feb 2020

Cyber Security Operating Model

11th CDEF Meetup - 27 Feb 2020

Basic definition

What is an IT Operating Model?	IT Strategic Planning & Governance	IT Operating Model

	"What should IT be doing for the business ?"	*"How does IT structure itself to deliver on the strategy ?"*

- Creates an **integrated view** of how **IT services** will be provided

- Provides a **consolidated description** of each IT function and the underlying processes

- **Supported by a diagram** of how all elements will fit together

ITSP	Solutions to facilitate development of a company's statement of the future state IT vision it is building toward in terms of guiding principles, investment plans & priorities, sourcing, skills and governance. Strategy is reflected as a series of strategic initiatives , delivered through development of a sound IT operating model.
ITOM	Solutions to facilitate the transformation of IT structures necessary to deliver the strategy. Operating models address key characteristics of the IT function such as organizational structure, processes, roles & responsibilities, sourcing, locations, etc.

Operating Model Basic Components

Organization

- Organization structure, roles, and responsibilities
- Sourcing options (in, out, hybrid)
- Capabilities development and monitoring

Governance

- Governance model (e.g steering committee)

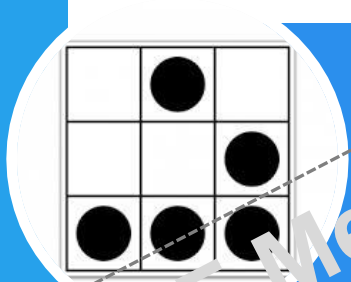**Service Management**

- Service offering and delivery

Security Architecture *

"*Plan your execution. Execute your plan.*"

- Anonymous

Cyber Transformation in OT Environment [redacted]

Put the foundation as input

Key Inputs

- Business Objectives
- Audit Findings
- Risk Themes
- Threat Landscape
- Current projects
- Goal cards - examples

From strategy to execution (3 years)

Control Baseline – Goal X

- NIST Cybersecurity Framework
- XYZ Risk Profile Process Control Domain
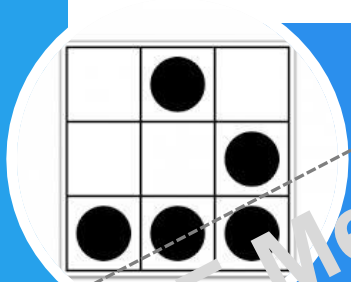- XXX Process Control Integrity Framework

- Benefits
- Success Factors
- Metrics
- How to Achieve the Goal
- Dependencies

Ensure fix the basics done well

Core Assessment

Site Survey Details	Assessment Categories	Process-based Assessment
▪ Workstations and Servers ▪ Network assets	▪ Policies, Procedures, Standard ▪ Physical Security ▪ Network Security ▪ Host Security ▪ Safety ▪ OT/ICS/SCADA System ▪ Asset Lifecycle	▪ > 10 Process Domain ▪ Risks for each Process Domain

Organizational Maturity & Capability

Process Safety

General Control & Process Control Audit

11th CDEF Meetup – 27 Feb 2020

Closing

*"**Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat.**"*

- Sun Tzu

Thank You

https://medium.com/@proferyk

https://www.slideshare.net/proferyk