

# PROCESS IMPROVEMENT FOR COMMON CRITERIA EVALUATION

in Malaysian Context



Siti Fatimah Abidin (Presenter)  
Norahana Salimin

Analyst, MySEF  
Security Assurance, CyberSecurity Malaysia  
Tuesday, 27<sup>th</sup> September 2011

# Content

---

- Introduction
- Overview
- Analysis and discussions
- Conclusion

# INTRODUCTION

## “Product evaluation and certification”

One of many ways to demonstrate that your ICT product or system is reliable and recognized



## COMMON CRITERIA (CC)

# Introduction

---

“ Although CC has become an international standard of IT security evaluation, it still contains many issues and limitations ”

**Changying Zhou & Stefano Ramacciotti**



# Introduction

---

## CC Evaluation



Higher assurance  
longer duration,  
higher cost



Outdated  
evaluation result



Outdated  
vulnerability  
assessment result

# Introduction

---

- Key aspect for process improvement to reduce evaluation duration:
  - Project management
  - Client collaboration
  - Product technology, development and testing methodologies
  - Evaluator expertise

# OVERVIEW

# ESP2 Project

---

- **Financial assistance** was provided by CyberSecurity Malaysia under the **Economic Stimulus Project 2 (ESP2)** for eligible Small Medium Enterprises (SMEs) developing ICT product **to obtain CC** certification through Malaysian Common Criteria Evaluation and Certification Scheme (MyCC)
- **16 products** has been accepted under ESP2 project for EAL 1 and EAL 2
- Targeted to be evaluated **by end of 2010**

# ANALYSIS AND DISCUSSIONS

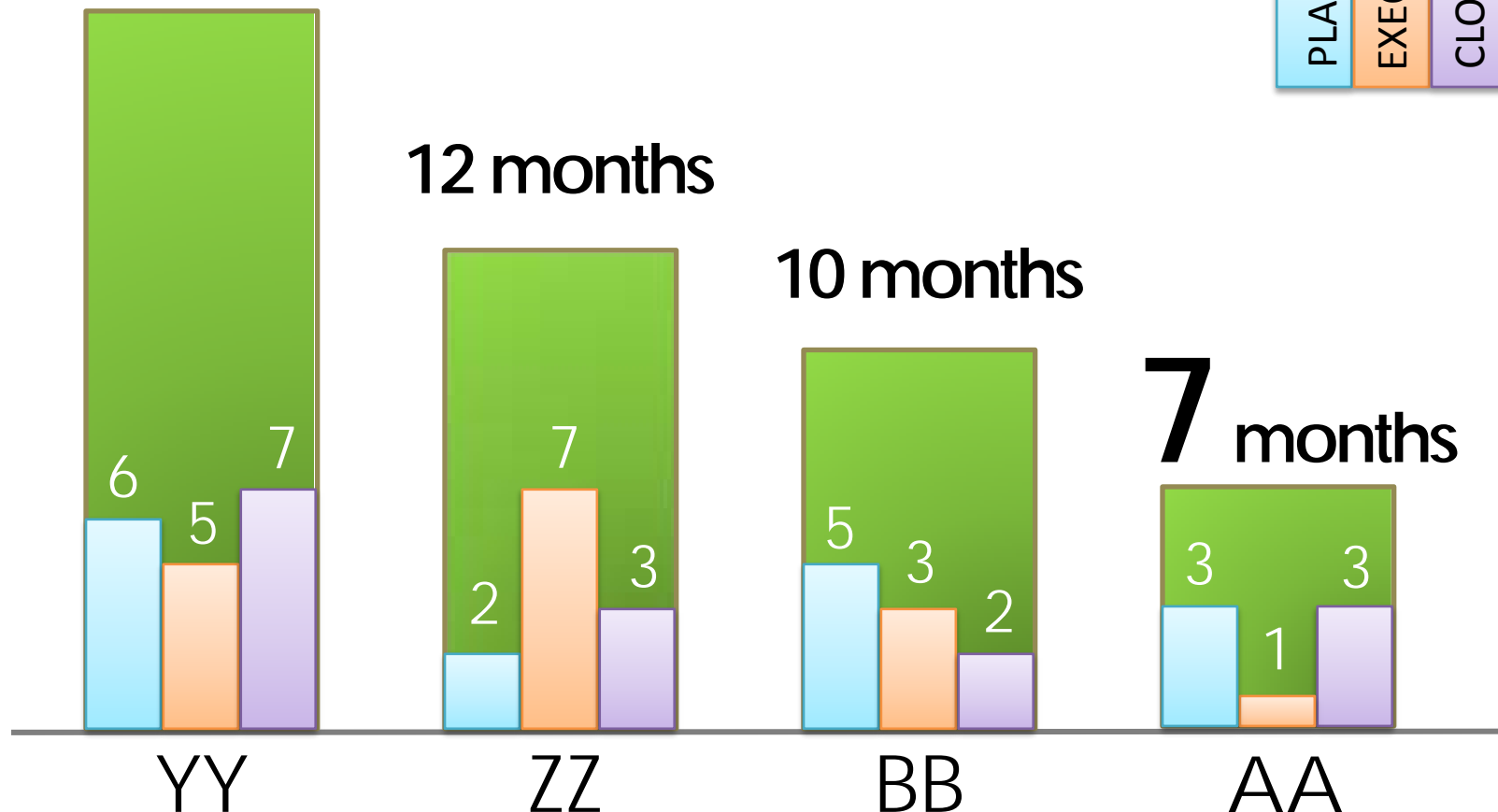
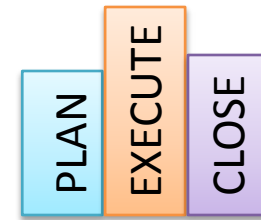
# Project Analysis

- Project selection
  - The shortest 2 :  
Project AA & BB
  - The longest 2:  
Project YY & ZZ
  - EAL 1

#	Project Code	EXE phase (months)	EAL
<b>1</b>	<b>AA</b>	<b>1</b>	<b>1</b>
<b>2</b>	<b>BB</b>	<b>3</b>	<b>1</b>
3	CC	3	1
4	DD	3	1
5	EE	3	1
6	FF	4	2
7	GG	4	2
8	HH	4	2
9	JJ	4	1
10	KK	4	1
<b>11</b>	<b>YY</b>	<b>5</b>	<b>1</b>
12	LL	5	2
13	MM	5	2
14	NN	5	2
15	PP	5	2
<b>16</b>	<b>ZZ</b>	<b>7</b>	<b>1</b>
17	QQ	21	3
18	RR	24	4

# Duration of Evaluation Project

**18 months**



# Key Aspects for Process Improvement

---

- Project Management
- Client Collaboration
- Product Technology, Development and Evaluator Expertise
- Testing Methodologies

# Project Management



**18** evaluation projects (concurrent)

**5** projects per evaluator



Tight schedule



Delay

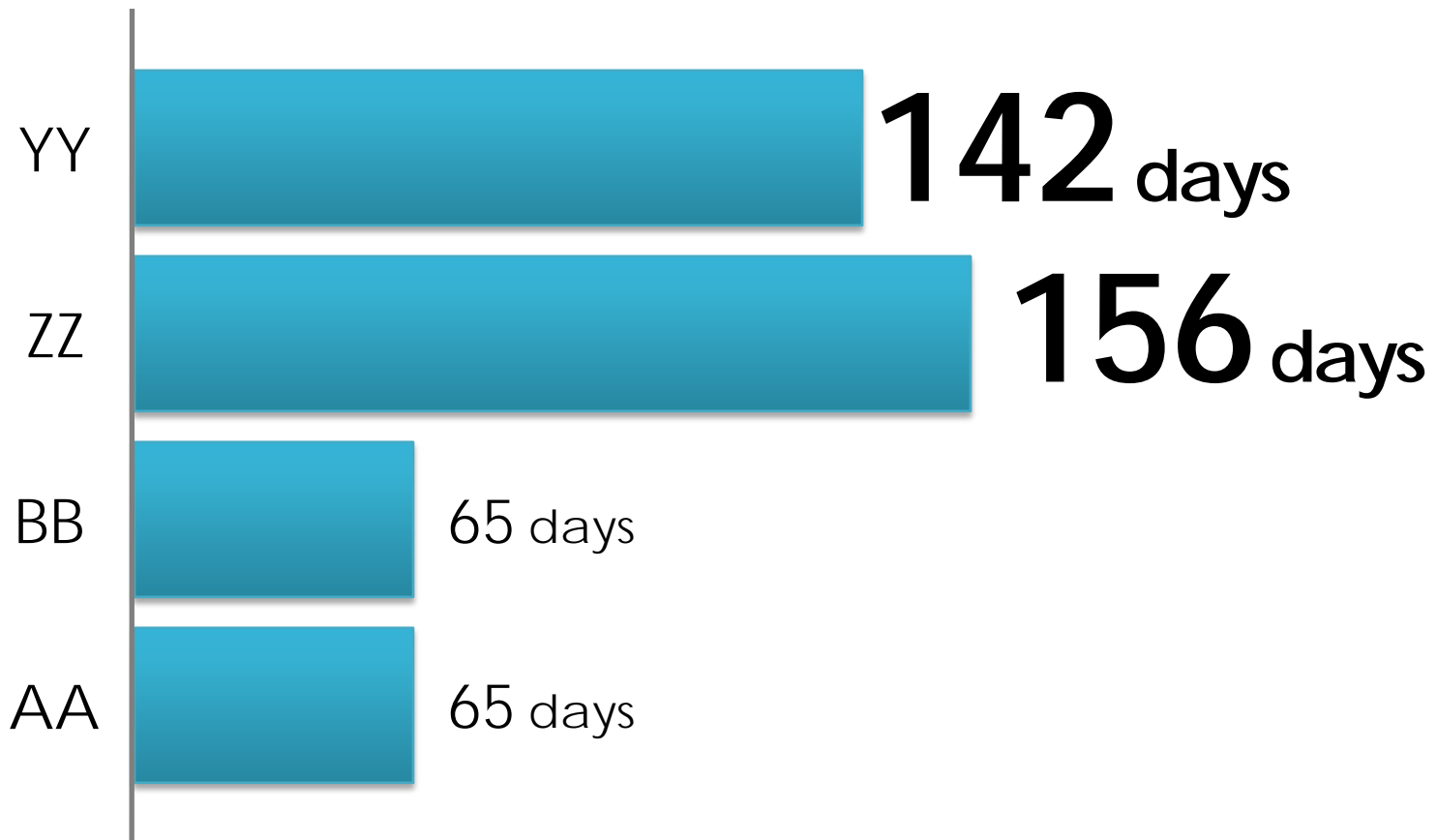
## Process improvement



Reassign other evaluators to  
critical project

# Client Collaboration

Total of days taken by developer/consultant to respond



# Client Collaboration

**Late respond by  
developer/consultant on  
issues raised by evaluator**



commitment to other  
business activities



not understand  
clearly on the issue

# Client Collaboration

## Process improvement



provide internal  
consultant



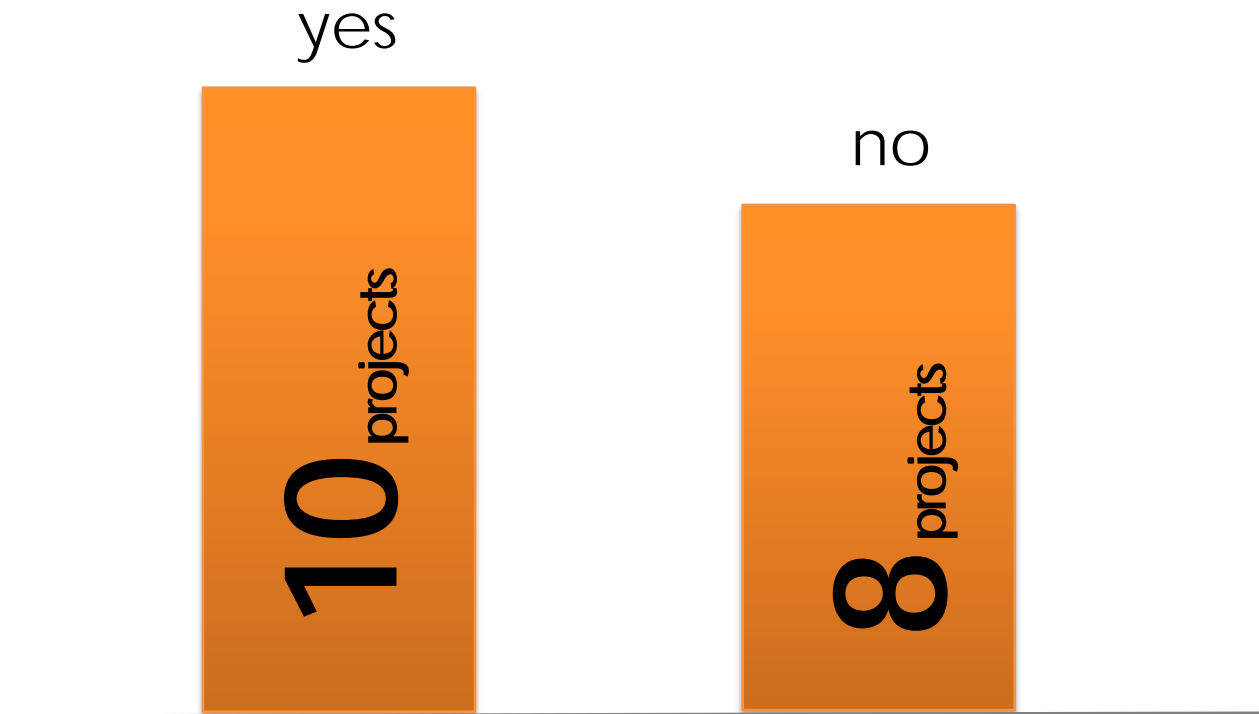
direct discussion with  
developer and/or  
consultant



take legal action as  
per stated in service  
agreement

# Client Collaboration

Direct discussion with developer/consultant



# Product Technology

**Niche technology**  
requires extensive research during  
evaluation



Smart card



Biometric



Cryptography

# Product Technology

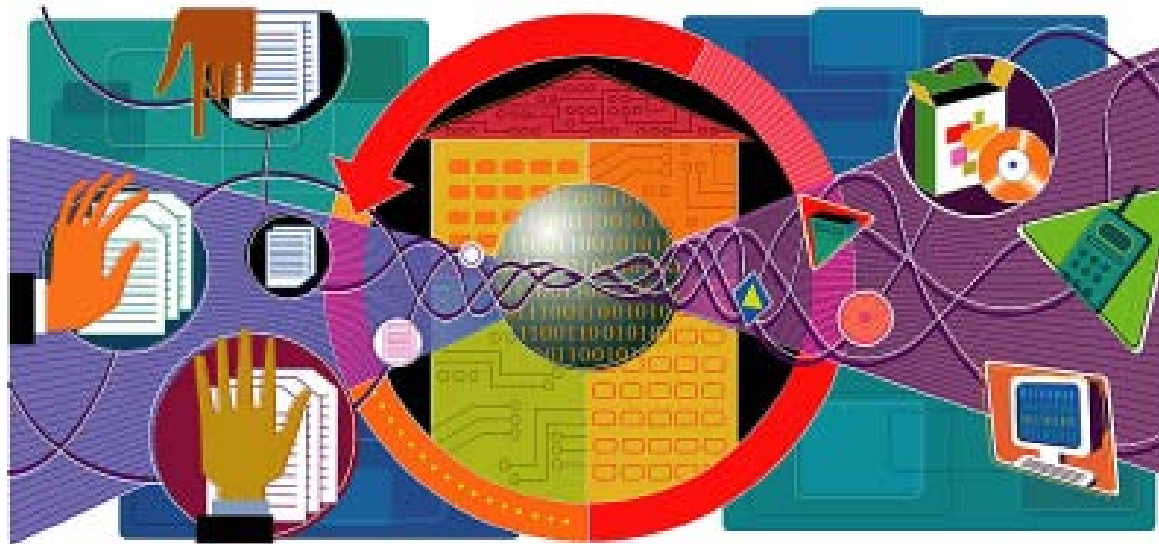
## Process improvement



Engage subject matter expert to provide knowledge in terms of product technology

# Product Development

## Evaluation concurrent with product development



## Process improvement



Follow up developer progress every 2 weeks to ensure no delay to the project

# Testing Methodologies

---

**Much effort on test plan development if product type has not yet encountered by lab**



# Testing Methodologies

## Duration of AVA phase





# Testing Methodologies

---

- Common Evaluation Methodology (CEM) is a guideline for evaluators in executing CC evaluation.
  - Consist of requirements of the product or product documentation for the product to be certified
  - repetitive evaluation effort as several requirements are interrelated and interdependent.

# Testing Methodologies

---

## Common Evaluation Methodology (CEM)



Repetitive evaluation effort;  
as several CEM requirements  
are interrelated and  
interdependent.

# Testing Methodologies

---

## Process improvement

Summarized all interrelated  
and interdependent  
requirement in table format  
(ASE, AGD, ADV, ATE)

# Testing Methodologies

Sub system	SFR-enforcing supporting non-interfering	Behavi or	TSFI	SFR	Purpose	Method of use	Admin	Test case	params
CPU	<u>FCS_COP</u> <u>FMT_LIM</u> <u>FPT_PHP</u>	Excutes opcodes fetched via the bus...	DATABUS	<u>FCS_COP</u> <u>FMT_LIM</u> <u>FPT_PHP</u>	Blah blah blah blah	bus	No		N/A
			RESET	<u>FCS_COP</u> <u>FMT_LIM</u> <u>FPT_PHP</u>		Reset line	No	42, 2501	N/A

Analysis of CC requirements in table format

# Summary

---

- **Project Management:**
  - Rearranged or reassigned evaluators to critical project which is expected to delay.
  - Sharing the information or lesson learned from test that has been conducted or feedback from certification body with other evaluators to avoid duplicating unnecessary effort.
- **Client Collaboration:**
  - Provides internal consultant among evaluators who were not involved in the respective project to assist developer resolve evaluation issues.
  - Organize direct discussion with developer and/or consultant to speed up resolving issue in EOR.

# Summary

---

- **Product Technology, Development and Evaluator Expertise:**
  - Engage subject matter expert for project on niche technology's product to speed up knowledge transfer.
  - Regular follow up developer progress if evaluation is concurrent with product development.
- **Testing Methodologies:**
  - Develop test plan template for AVA execution.
  - Record evaluation results in table format which covers requirement in ASE, ADV, AGD and ATE.

# CONCLUSION

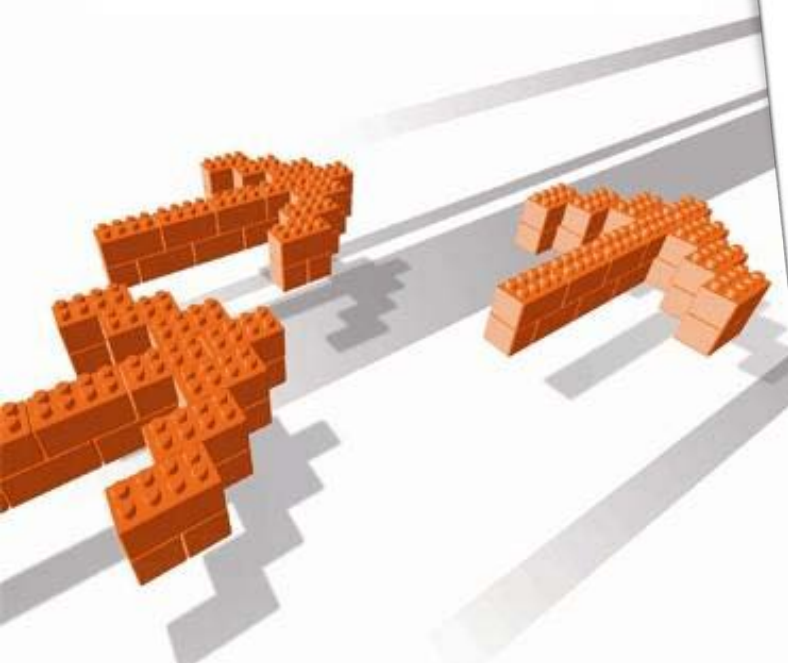
# Conclusion

---

- Common Criteria is a new initiative in Malaysia.
- Need improvement:
  - delivering evaluation service in a shorter period while not sacrificing the quality of evaluation results.
- Future research may be conducted to improve evaluation duration and cost in terms of testing methodologies using site certification and developing evaluation evidence template which contain all CC requirements.

# Q&A





*Corporate Office:*  
**CyberSecurity Malaysia,**  
Level 8, Block A,  
Mines Waterfront Business Park,  
No 3 Jalan Tasik, The Mines Resort City,  
43300 Seri Kembangan,  
Selangor Darul Ehsan, Malaysia.

T +603 8946 0999

F +603 8946 0888

[www.cybersecurity.my](http://www.cybersecurity.my)

# Thank You

