Penetration Testing

A Structured Approach

DEFCONPH Manila Beer Talk II

April 24, 2009

Discussion Agenda

- Introduction and Overview of Penetration Testing (PT)
- PT - Feasibility, Quality, Value and Limitations
- Business Models and the Bidding Process
- Project Management
- PT Methodologies and Tools
- Risk Management
- Communicating the Results
- Constraints, Challenges and Legal Issues

Introduction

- The objective of this presentation is to provide a meaningful perspective regarding penetration testing as a service.
- This presentation is focused on the elements beyond the technical process of conducting penetration testing.

Overview of Penetration Testing (PT)

What is Penetration Testing?

> *“A **method** of **evaluating the security** of a **computer system or network** by **simulating an attack from a malicious source.**” - Wikipedia*

Who are the Players?

Global Leaders

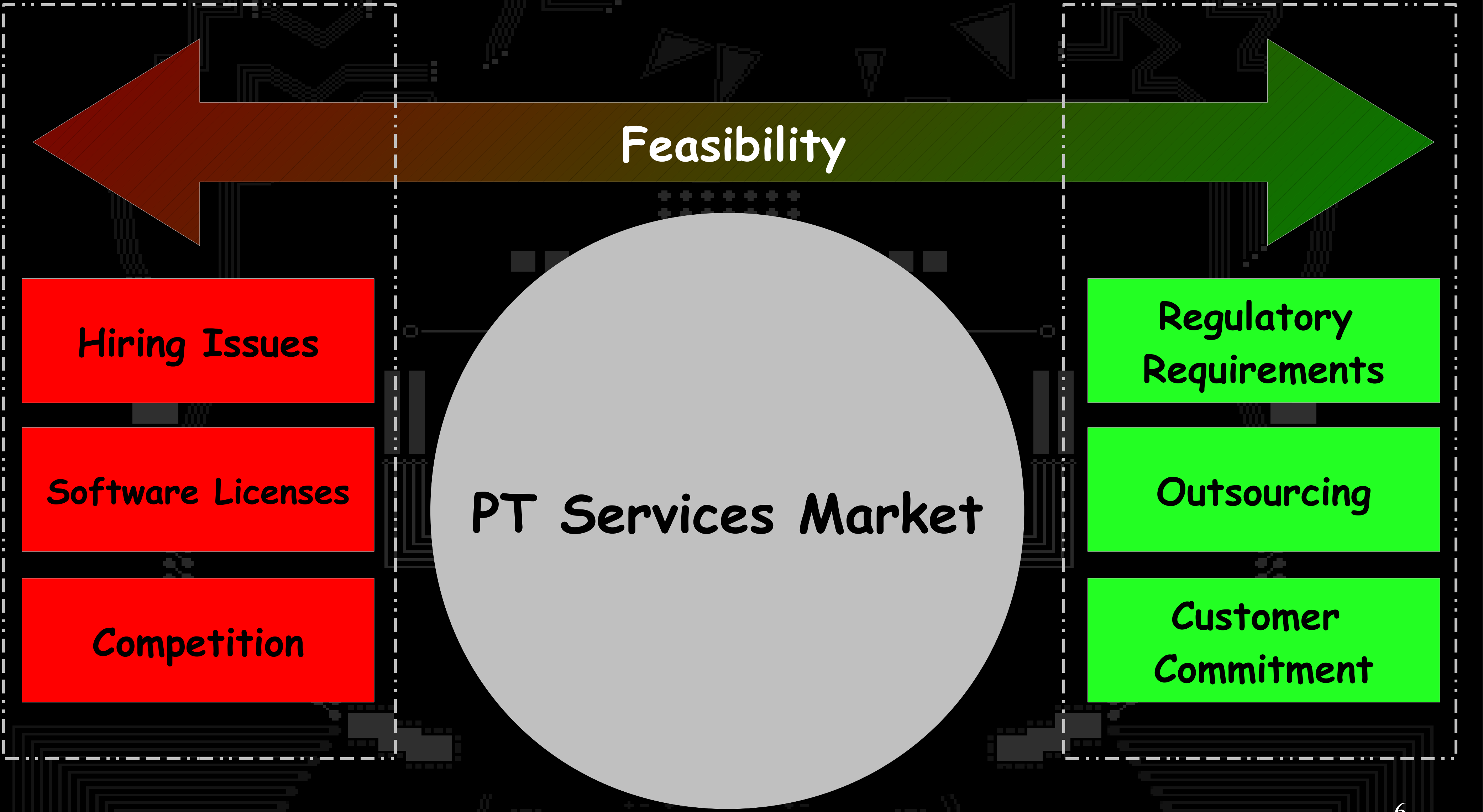
- Deloitte
- PWC
- E&Y
- Accenture

Source: The Forrester Wave™: Information Security And IT Risk Consulting, Q1 2009, Note that KPMG did not participate in this survey

Philippines

- IBM
- KPMG
- PWC
- E&Y
- Bitshield Security Consulting
- Laggui & Associates
- SeQure Technologies
- Verizon Business

PT - Business Feasibility



Feasibility

Hiring Issues

Software Licenses

Competition

PT Services Market

Regulatory Requirements

Outsourcing

Customer Commitment

PT – Quality of Service

Differences in the Quality of PT as a service depends on:

- The extent to which the penetration test caters to the client's technical and business environment or situation
- How much time and resources are spent on detecting vulnerabilities related to IT components included in the Scope
- How creative the penetration tester's approach and methodology is

PT – Value of Service

What value does your service bring to my business?

Peace of Mind?

Identify my control weaknesses?

Compliance with Regulatory Requirements?

Improve my Security Posture?

THE HELPLESS CLIENT

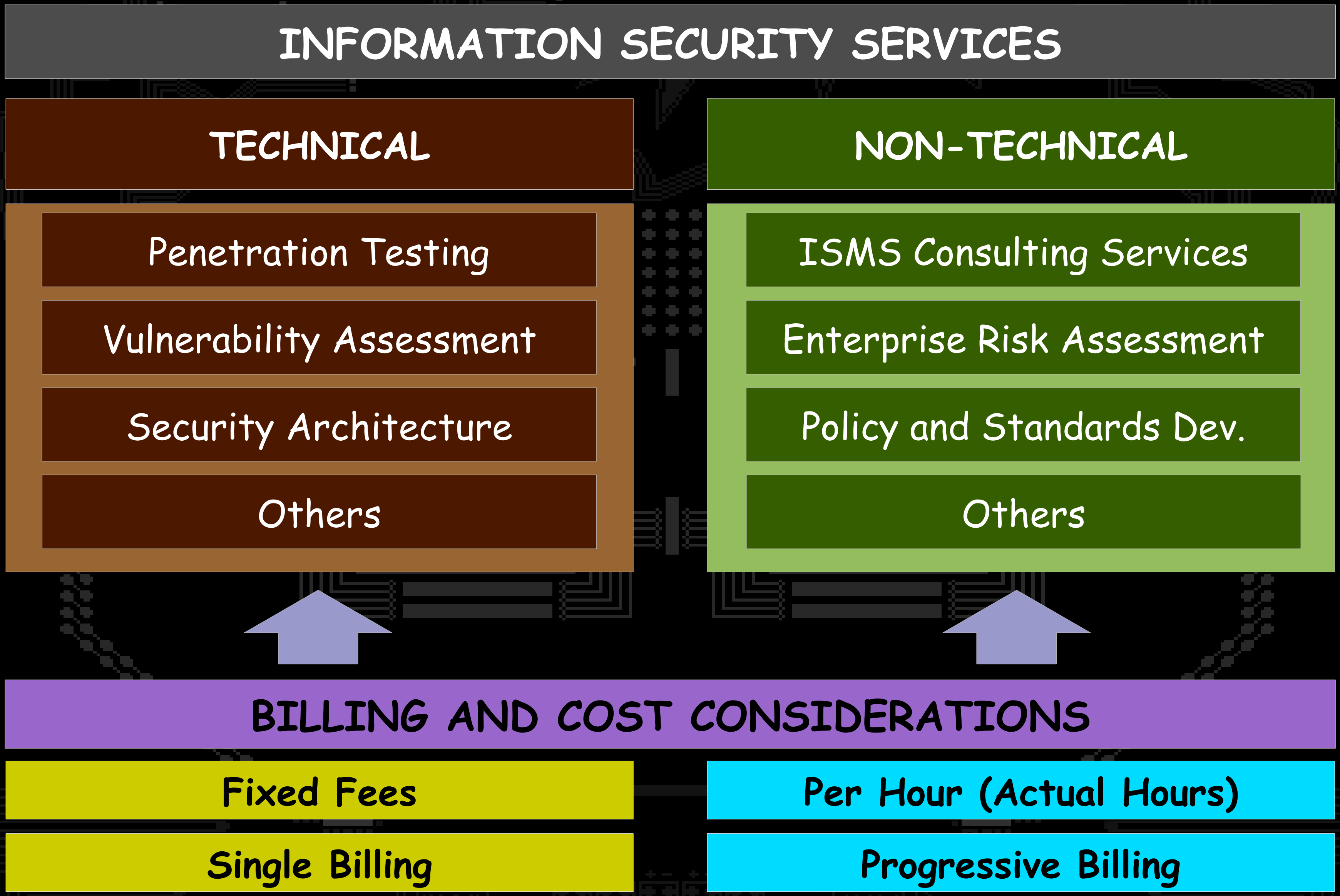
PT – Limitations

- A Penetration Test only reflects the situation at a **particular point in time** and cannot provide assertions about the company's security posture that are valid in the future.
- A thorough Penetration Testing **does not guarantee that a successful attack will not occur**, *but it may reduce the probability of a successful attack.*

PT – Limitations, Cont.

- A Penetration Test **<u>is not a substitute</u>** for a general security policy or other IT security-related testing

Business Models



INFORMATION SECURITY SERVICES

TECHNICAL

- Penetration Testing
- Vulnerability Assessment
- Security Architecture
- Others

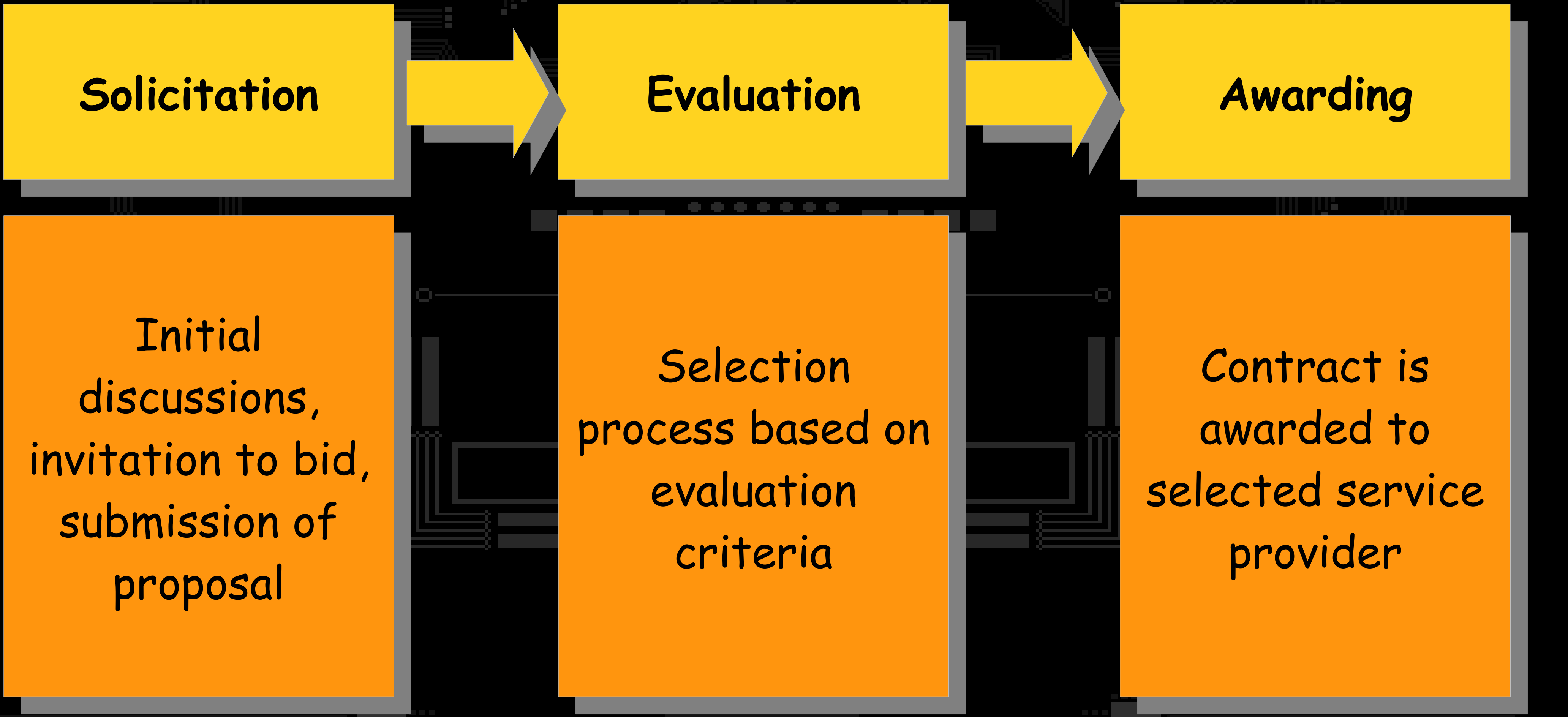
NON-TECHNICAL

- ISMS Consulting Services
- Enterprise Risk Assessment
- Policy and Standards Dev.
- Others

BILLING AND COST CONSIDERATIONS

- Fixed Fees
- Single Billing
- Per Hour (Actual Hours)
- Progressive Billing

The Bidding Process



Solicitation

Evaluation

Awarding

Initial discussions, invitation to bid, submission of proposal

Selection process based on evaluation criteria

Contract is awarded to selected service provider

The Bidding Process, Cont.

- First Things First: ***Understand the Business of your Client***
- Proposal Preparation:
  - Initial discussion about the Scope, Fees and other relevant matters
  - Study and understand the Request for Proposal (RFP) and its Terms of Reference (TOR) - *Strictly follow the RFP specifications*

The Bidding Process, Cont.

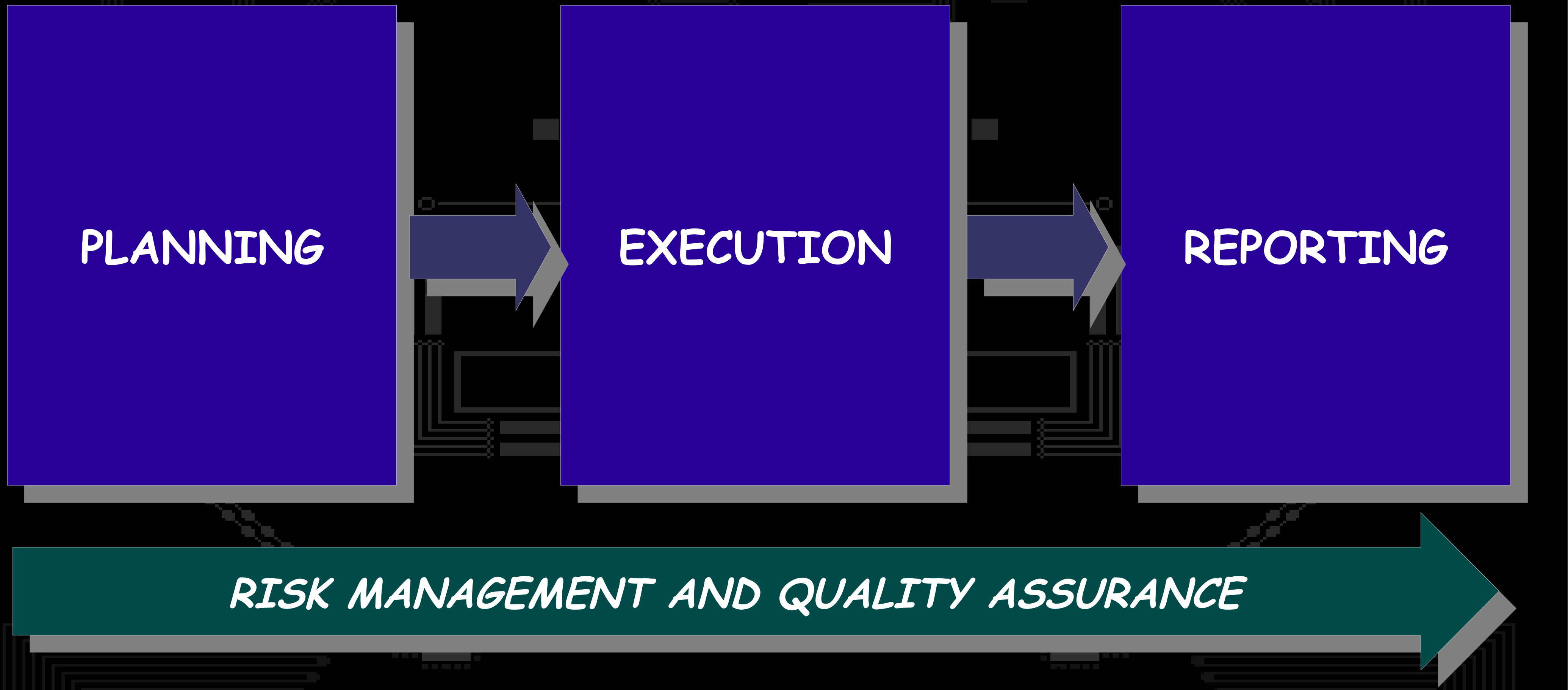
- Sample bidding eligibility requirements:
  - Latest audited financial statements
  - Predefined qualification requirements for both the service provider and the professionals involved
  - Client references and previous engagements

Professional Qualifications

- **Demonstrated Professional Integrity**
- Required number of years – information security experience of the service provider and its professionals
- Education and certification requirements of professionals

Project Management

Security Project Management - Approach



PLANNING

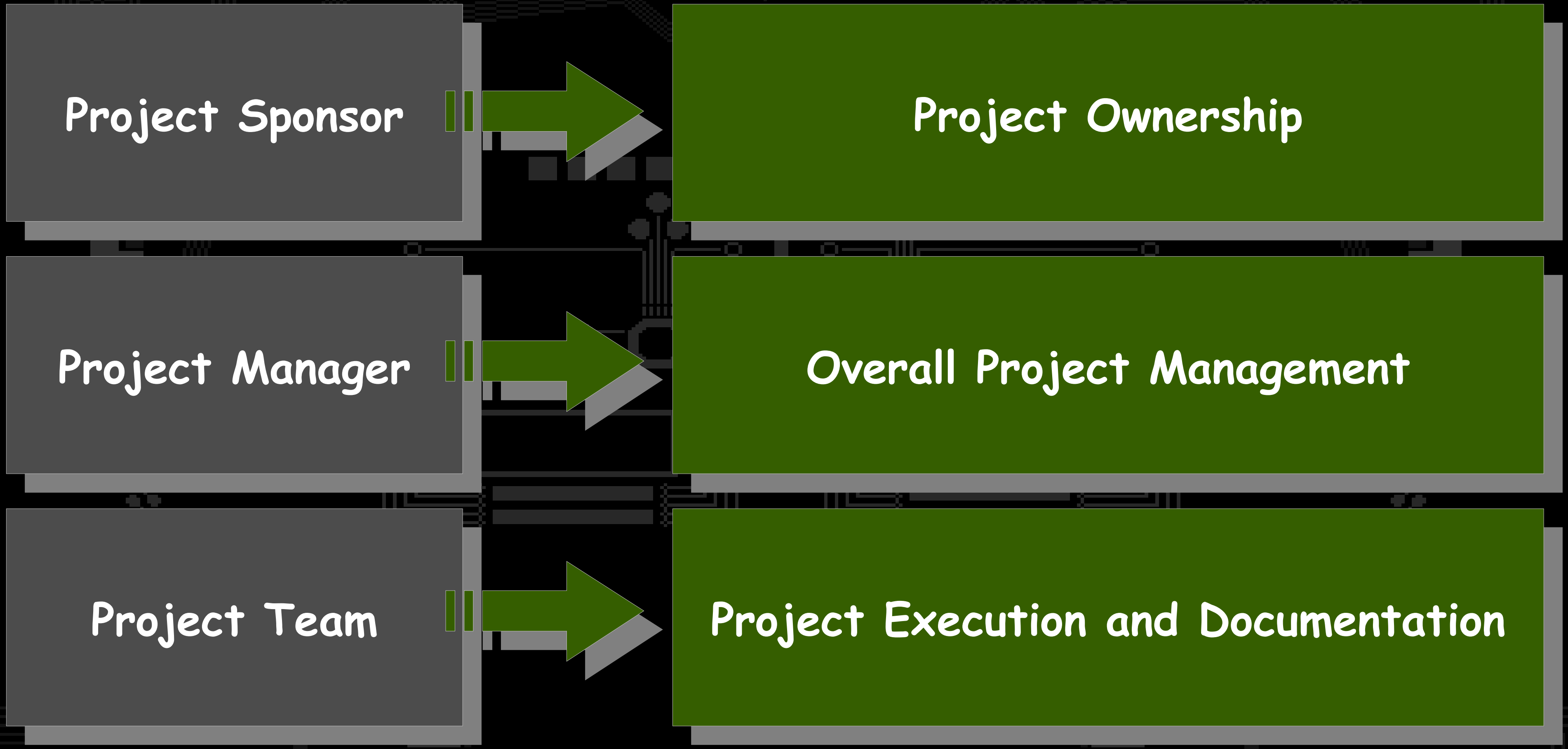
EXECUTION

REPORTING

RISK MANAGEMENT AND QUALITY ASSURANCE

Project Management, Cont.

Security Project Management - Organization



Project Sponsor → Project Ownership

Project Manager → Overall Project Management

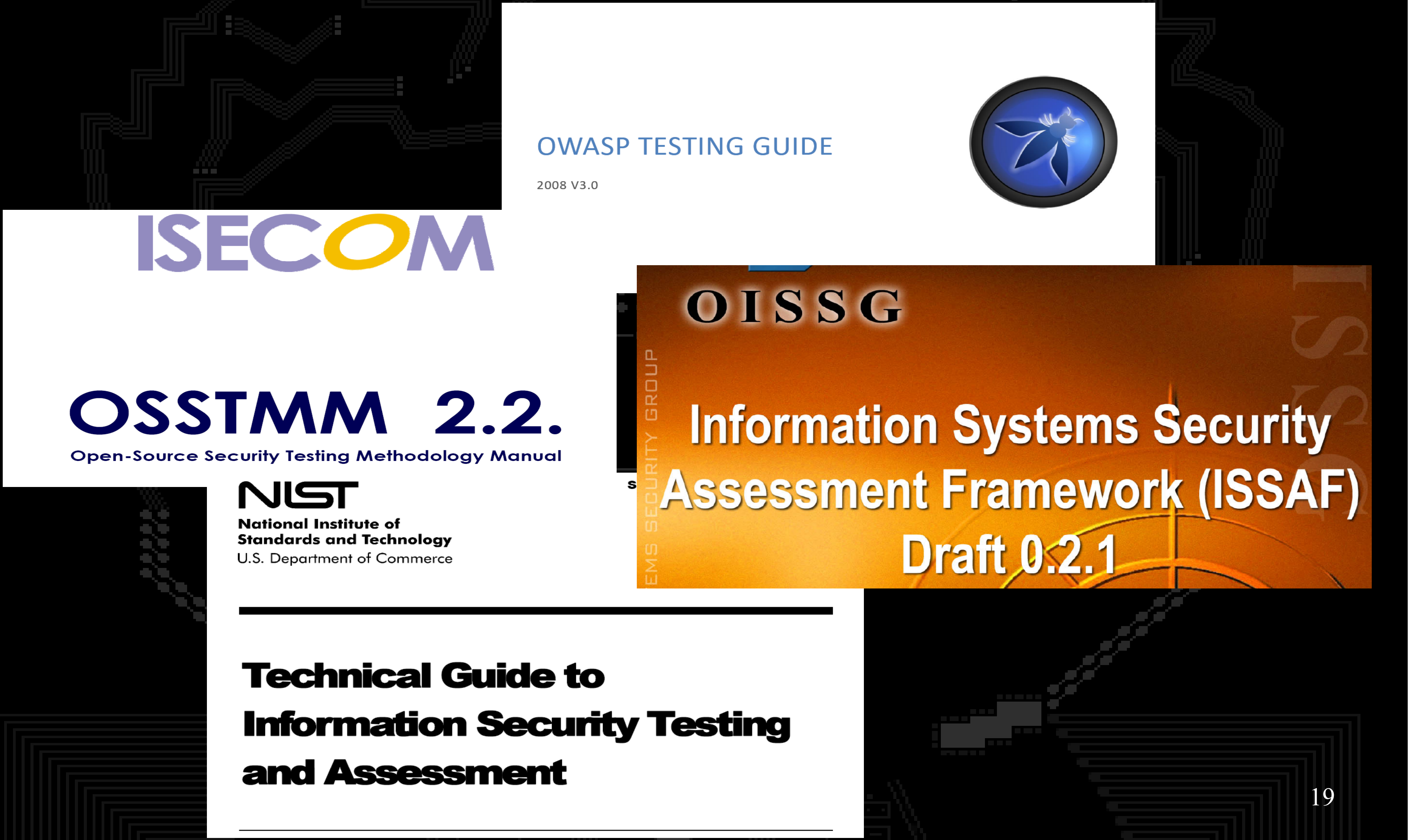
Project Team → Project Execution and Documentation

Service Provider Responsibilities

Abiding to contractual obligations:

- Maintain confidentiality of information
- Comply with relevant regulations, professional standards and ethics
- Address authorization issues and know your boundaries
- Document penetration test procedures and its results
- Perform penetration test with **Due Professional Care**

PT Methodologies



OWASP TESTING GUIDE

2008 V3.0

ISECOM

OSSTMM 2.2.

Open-Source Security Testing Methodology Manual

OISSG

EMS SECURITY GROUP

Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1

NIST

National Institute of Standards and Technology
U.S. Department of Commerce

Technical Guide to Information Security Testing and Assessment

PT Tools

- Why do we use tools?
  - Efficiency
    - More output in less time and at lower cost
  - Completeness and Accuracy

*"Tools are just tools, nothing can replace a penetration tester's **Competence and Professional Judgment.**"*

Risk Management

Murphy's law – *"Anything that can go wrong will go wrong"*

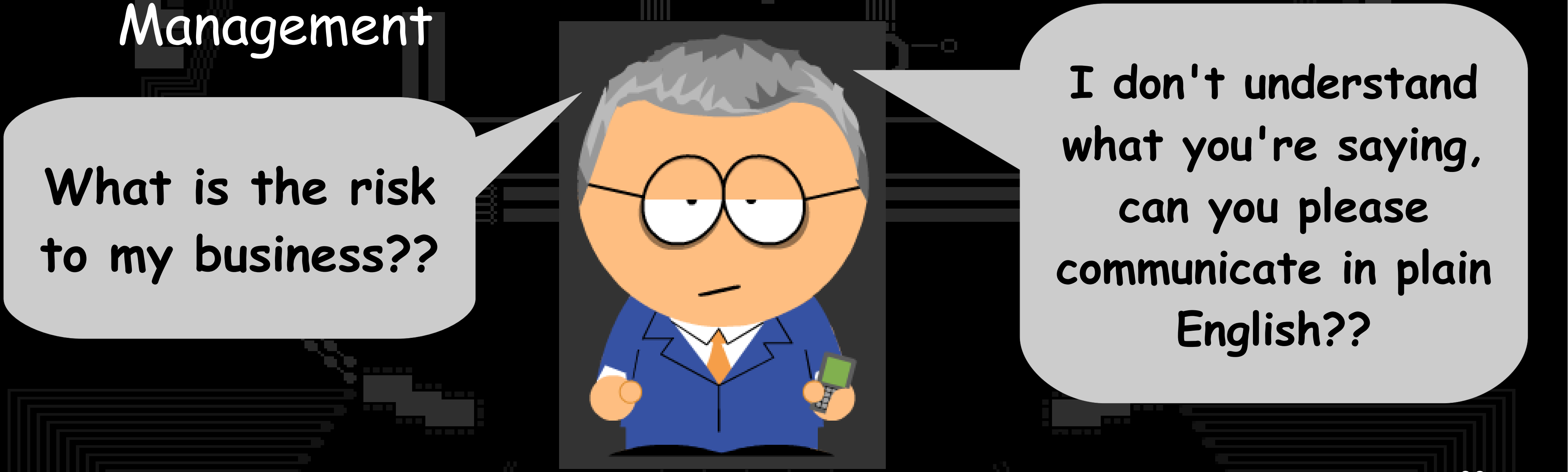
The client should recognize the Risk that PT activities may bring down their system even within a controlled environment.

Manage the Risk:

Strictly follow authorization protocols and implement precautionary measures - *Practice **Due Professional Care***

Communicating the Results

- The result of a penetration test should be more than just a list of existing vulnerabilities and should suggest solutions for their elimination.
- Presentation and submission of final report to Management


What is the risk to my business??
I don't understand what you're saying, can you please communicate in plain English??

THE HELPLESS CLIENT

Constraints and Challenges

- Client Management – Building Trust and Rapport
- Lack of necessary information to reasonably provide the service
- Scope Creep and Limitations

Constraints and Challenges, Cont.

- Third Party Involvement – Extranet PT
- Accidental Business Interruption:
  - Exploit code execution – possible server crashes (External and Internal)
  - MITM attacks – possible network downtime (Internal)

Legal Issues

What are the legal regulations and principles that the penetration tester should observe when conducting penetration tests and which should be clarified with the client prior to testing?

Questions?

Thank you