Global Standards Information

Conformity Assessment in the Information Technology Sector

Information **S**ecurity and **P**rivacy **A**dvisory **B**oard

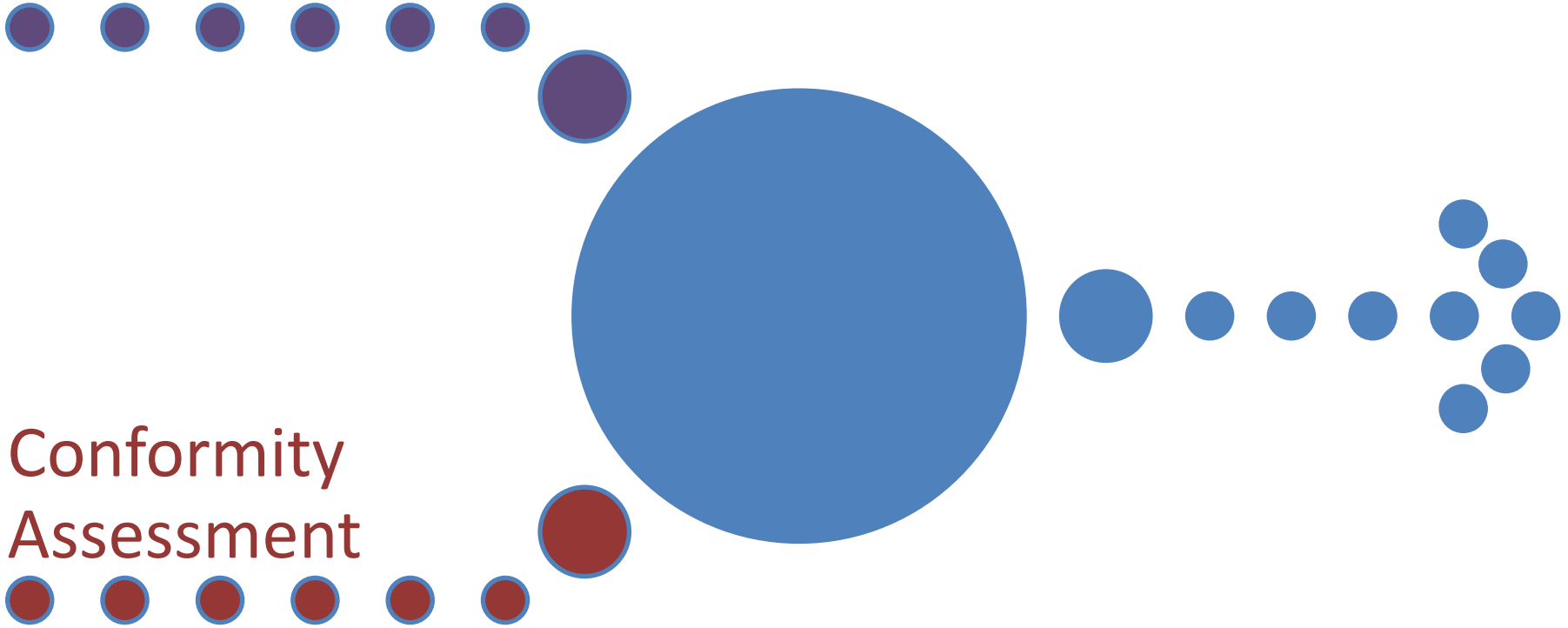
June 2012

Conformity Assessment

"demonstration that specified requirements relating to a product, process, system, person, or body are fulfilled"

- ISO/IEC 17000

Information Technology



Conformity Assessment

The Parties – who done it?

First Party – seller or manufacturer

Second Party – purchaser or user

Third Party – independent entity

Government

Types of Conformity Assessment

- Supplier's Declaration of Conformity (SDoC)
- Inspection
- Testing
- Certification
- Registration
- Accreditation

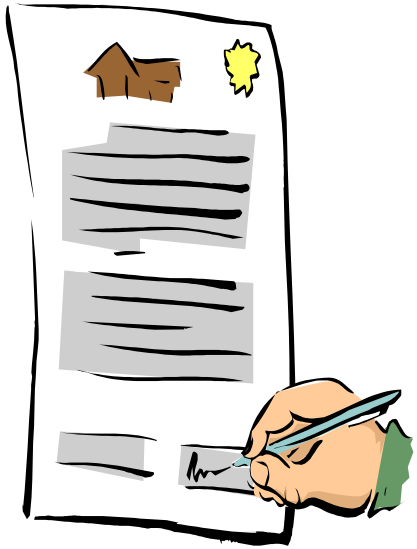
- ISO/IEC 17050 parts 1 and 2
- ISO/IEC 17020
- ISO/IEC 17025
- ISO/IEC Guide 65
- ISO/IEC 17021
- ISO/IEC 17011

Supplier's Declaration of Conformity (SDoC)

1st Party
2nd Party
3rd Party

Characteristics

- Used when low product risk
- Penalties for noncompliant products
- Effective recall system



Examples

- ISO/IEC 17050

Certification

1st Party
2nd Party
3rd Party

Characteristics

- Used when moderate – high product risk
- More expensive
- Surveillance

- ISO/IEC GUIDE 65

Examples

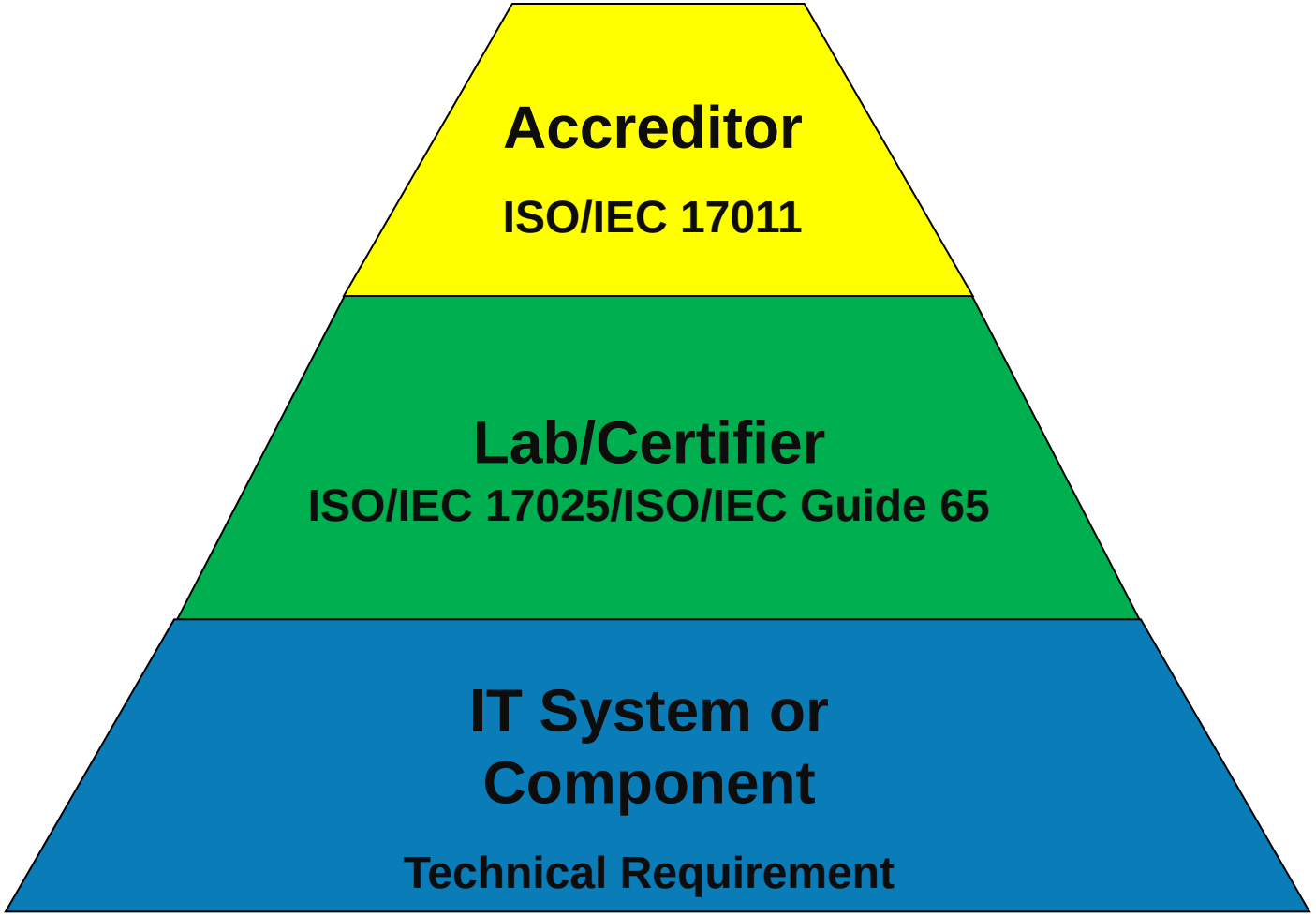
Accreditation

1st Party
2nd Party
3rd Party

Characteristics	Examples
• Confidence in Competence	NVLAP® ANAB ACCREDITED

- ISO/IEC 17011

Conformity Assessment Hierarchy



IT System Attribute in Need of Confidence

- *Function – IPV 6, E Health Records…*
- *Interoperability – WiFi, E Health Records…*
- *Portability – Cloud Services…*
- *Security – SmartGrid, E Health Records, Cloud Services…*
- *Other Attributes?*

Research Needs to Support Confidence

- *Standards and Requirements*
- *Test Methods and Tools*
- *Conformity Assessment Approaches*

and an **Effective** Business Case

Thank You

Gordon Gillerman

Standards Services

National Institute of Standards and Technology

gordon.gillerman@nist.gov

301-975-8406