

All in One Third Party Information Assurance

A tool for better Risk Management

Michel Godet and Metrici UK

Agenda

- **Due diligence requires**
 - Intelligence
 - Coherence
 - Sustainability
- **All in One**
 - A powerful platform for risk and compliance intelligence
 - Building blocks capture commonality and measure progress
 - Report impact on relationship with 3rd parties
 - Attention to root causes and highest priorities

3rd Party Information Assurance

- **Why?**
 - **Reduce risk**
 - Contract Due diligence
 - **Improve compliance**
 - Audit
 - Best practices
 - Regulation
 - **Madoff.**

Due Diligence Process

- **Actionable intelligence**
- **Issue tracking**
- **Impact modeling**

Risk & Compliance Intelligence

- **Risk management**
 - Monitored and managed?
- **Policies and procedures**
 - Adequate?
 - Up to date?
 - Understood
- **Controls**
 - Implemented and effective?
- **Performance**
 - Compliance met?
 - Issues with third partie relationships?

Coherence

- **Impossible to take right decision when intelligence is in silos**
 - FBI investigates
 - CIA analyzes
 - No one bothered to discuss impact of Saudis learning to fly but not how to land planes.

Sustainability

Going Green

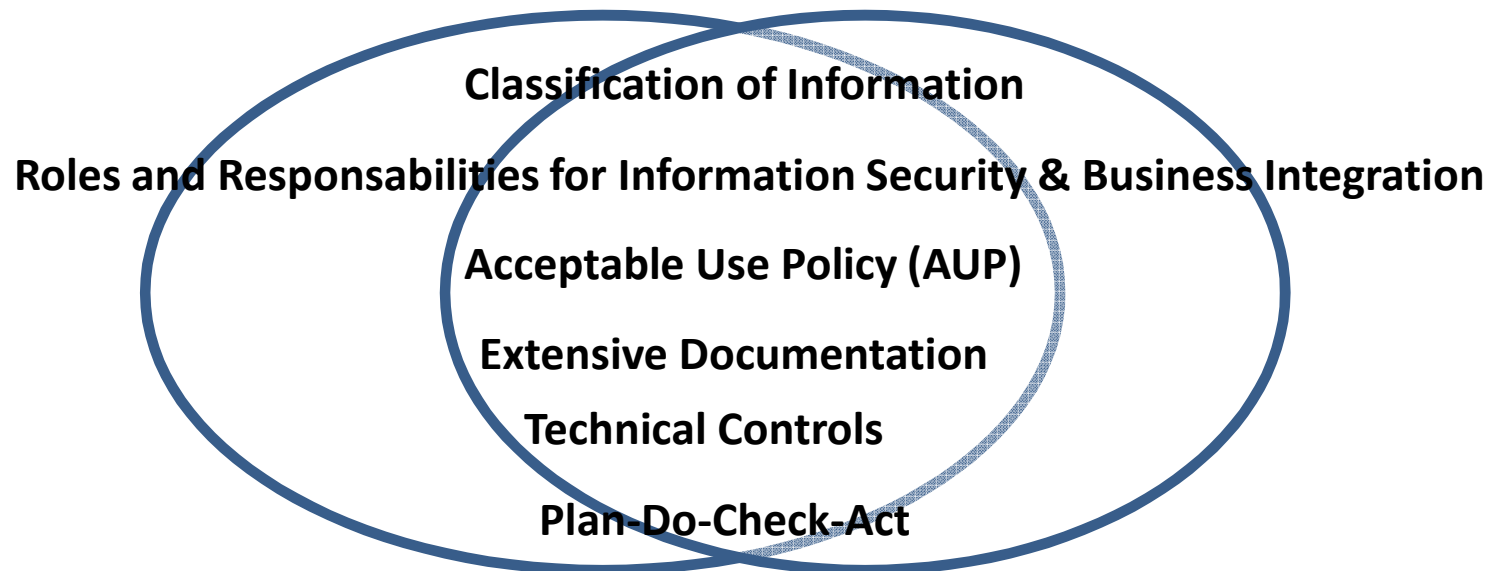
- **Senior executives must lead:**
 - Recycle controls and policies
 - Don't throw out previous work
 - Abstain from NIH

Silos miss Commonality

- Most firms meet individual regulations as they appear
 - **Slicing** activities
 - **Duplicating** resources
 - Making it **extremely difficult** for board to invest in People, Technology and Processes

For Example: ISO 27001 & PCI DSS

- If a company is **ISO 27001 certified**, it is likely that many of the policies, practices and controls that **PCI DSS** requires are already implemented

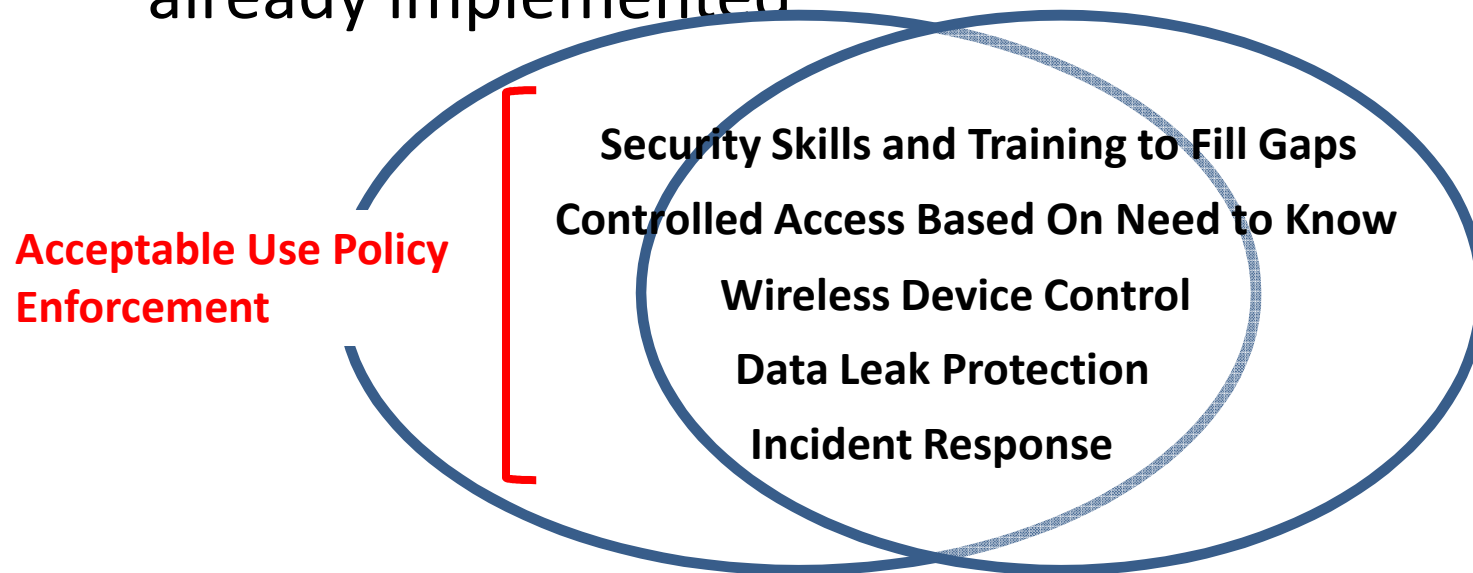


http://en.wikipedia.org/wiki/ISO/IEC_27001

http://en.wikipedia.org/wiki/PCI_DSS

For Example: ISO 27001 & CAG

- If a company is **ISO 27001 certified**, it is likely that many of the policies, practices and controls that **SANS Consensus Auditing Guidelines** requires are already implemented



http://en.wikipedia.org/wiki/ISO/IEC_27001

<http://www.sans.org/critical-security-controls/guidelines.php>

Capturing Commonality

- **Use holistic approach**

- Identify common issues and data
- Most standards and regulations are similar

- **For example,**

- **Red Flag Rules** are similar to
 - **HIPAA, Gramm-Leach-Bliley Act (GLBA) and Payment Card Industry (PCI) Data Security Requirements when dealing with the risk of identity theft**

http://en.wikipedia.org/wiki/Red_Flags_Rule

http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

http://en.wikipedia.org/wiki/Gramm-Leach-Bliley_Act

All in One

- **Powerful platform**
 - Risk and compliance intelligence
 - Alert organization to issues that impact relationships with business partners, suppliers and customer

Intelligence Gathering

Risk management

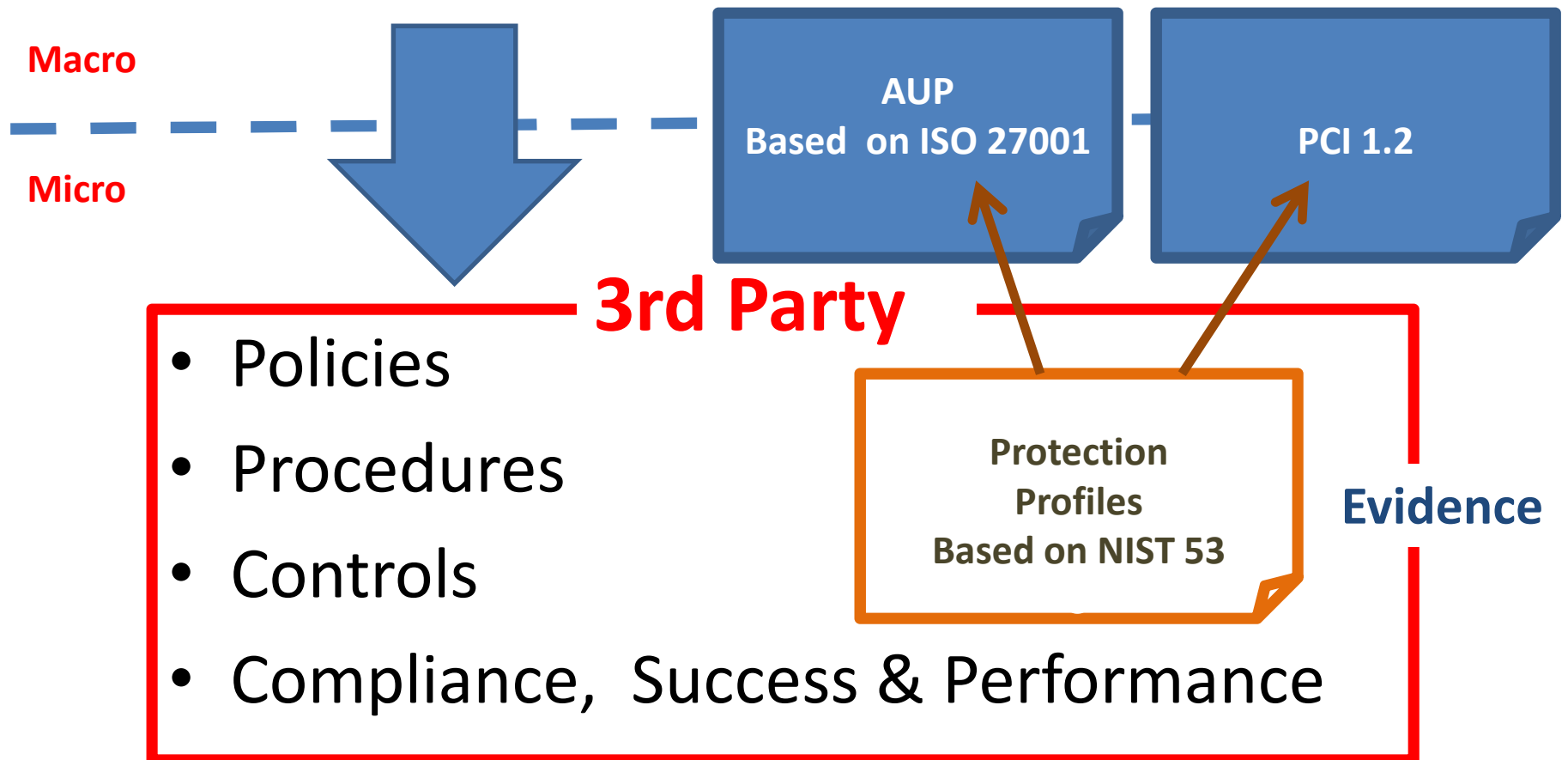


Building Blocks

- **Repository of assessment criteria**
 - Best practices
 - Detailed requirements
- **Assemble blocks to quickly make**
 - Assessment templates
 - Meet organization requirements

Assemble blocks

Risk management **Organizational requirements**



Measure Progress

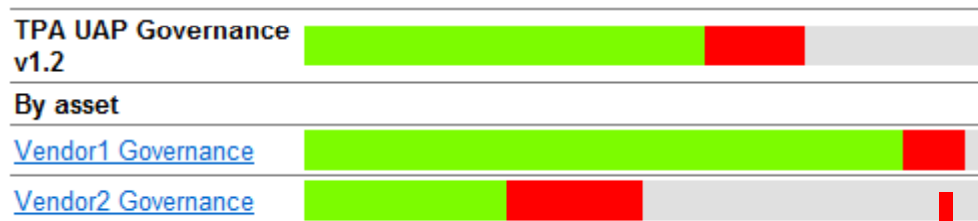
Level of Maturity/Metrics

Level of maturity					
Level 1	Level 2	Level 3	Level 4	Level 5	
Policy	Procedures	Procedures	P&C	P&C	
Developed	Developed	& Controls	Tested	Integrated	
		Implemented			
Types of Metrics					
Goals	Objectives	Implementation	Effectiveness	Impact	
Defined	Identified		& Efficiency		
			of security plans		

Reporting

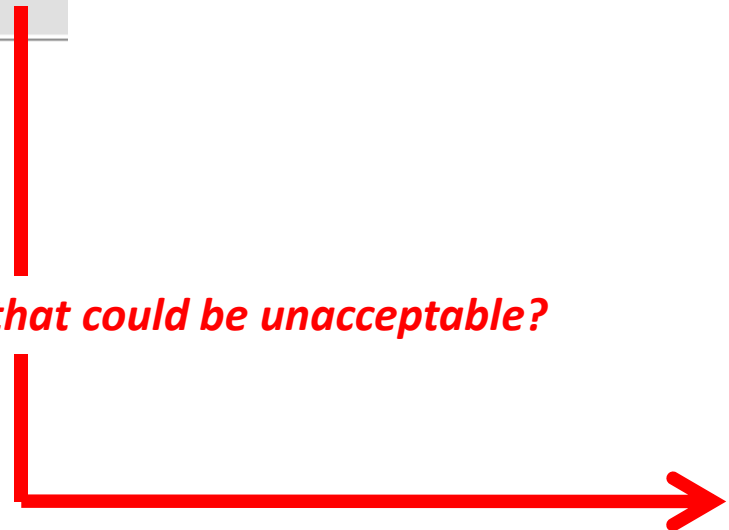
Understanding the general situation ...

- **Top down consolidations focused on what really matters for the organization as a whole**



Are compliance obligations being met?

Is there something that could be unacceptable?



Reporting

... Devil in the ...

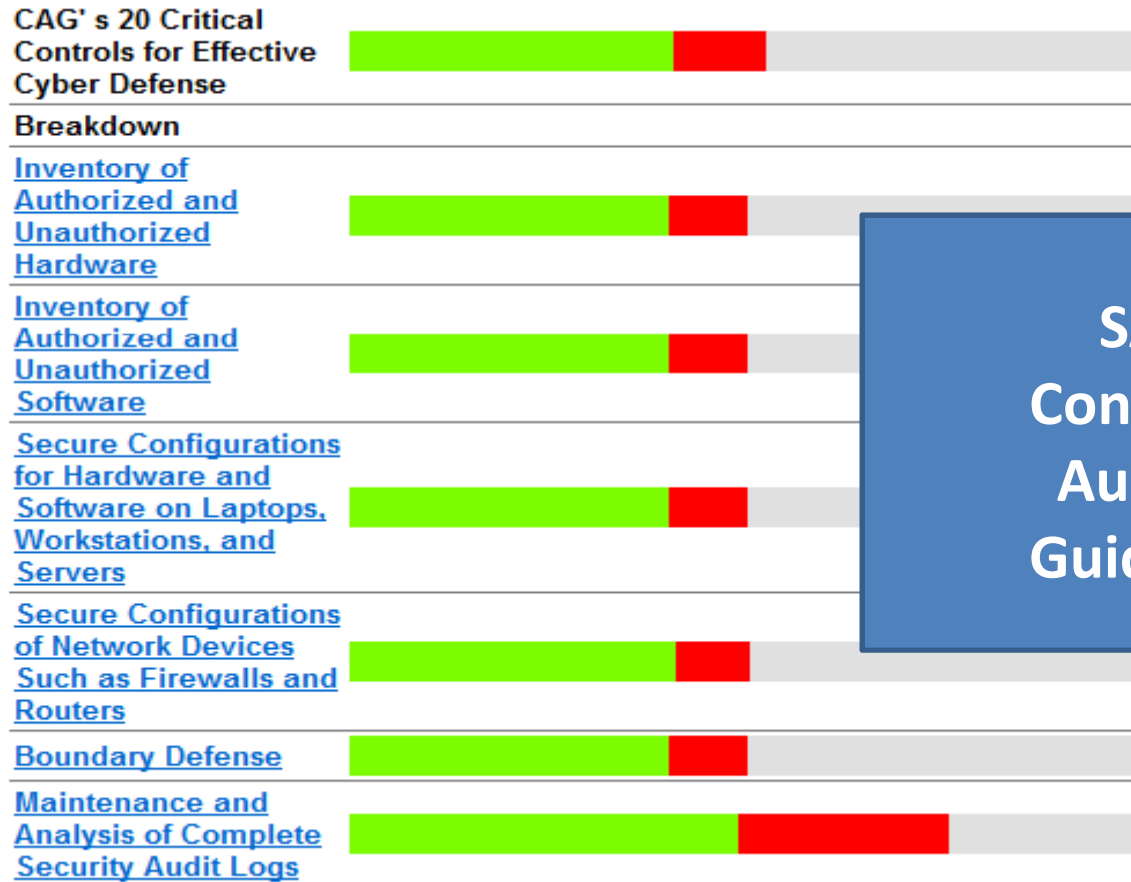
2 Protection Profile based on NIST SP 800-53 Controls

		Score	Coverage	Weight
Protection Profile based on NIST SP 800-53 Controls		73.5	91.6	50.0
Breakdown				
		79.1	98.9	2.8
		78.4	97.8	2.8
		80.6	99.3	2.8
		84.2	100.0	2.8
		80.6	99.3	2.8
		79.9	100.4	2.8
		79.9	100.0	2.8
		79.9	100.4	2.8
		79.9	100.0	2.8
		51.1	63.7	2.8
2.11 MP		79.9	100.4	2.8
2.12 PE		79.9	100.0	2.8
2.13 PL		47.8	60.1	2.8
2.14 RA		53.2	66.9	2.8
2.15 PS		79.1	100.4	2.8
2.16 SA		68.3	84.9	2.8
2.17 SC		60.4	74.5	2.8
2.18 SI		79.9	100.0	2.8

The Forest &
The Trees
On one single report

Reporting

... Prioritization



**SANS
Consensus
Auditing
Guidelines**