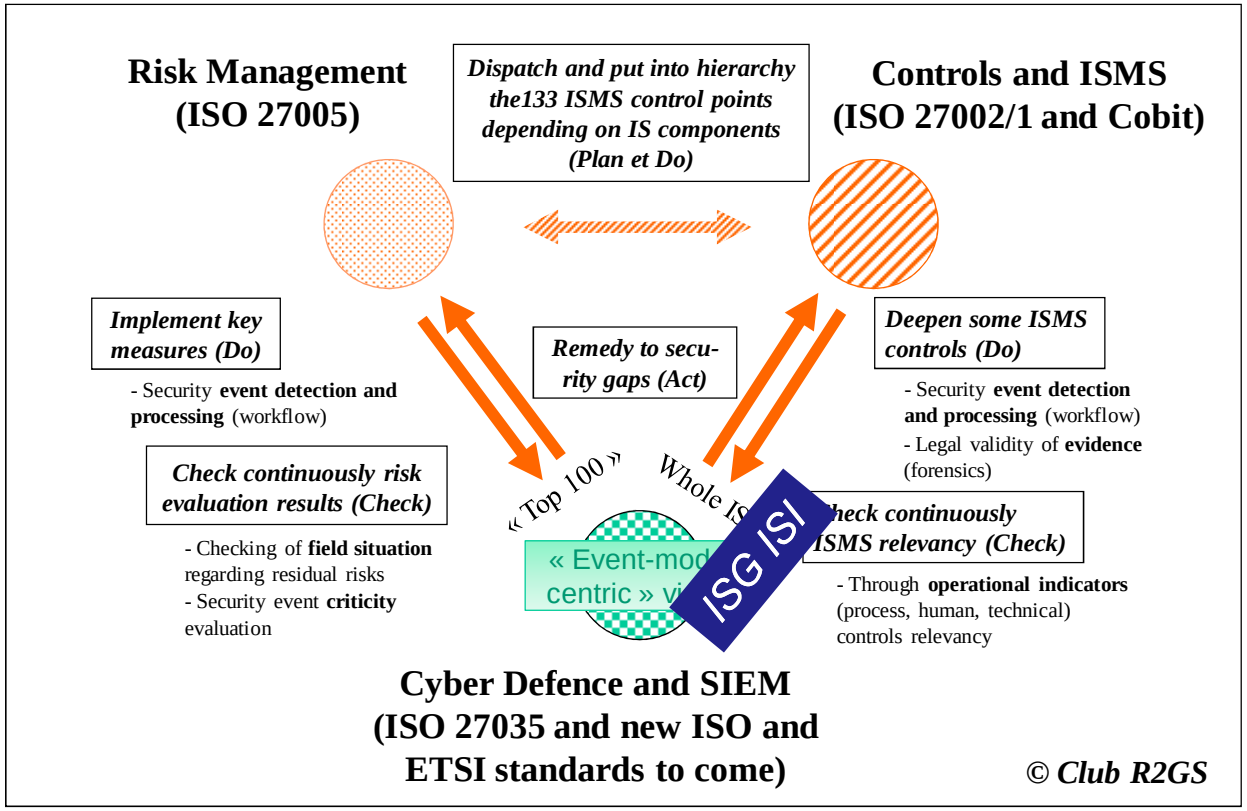
ETSI ISG ISI Standardization

(ISO SC27/ETSI Security joint meeting)

26 April 2013

Gerard Gaudin (G²C)
Chairman of ISG ISI

ISG ISI positioning against Risk Management and ISMS fields

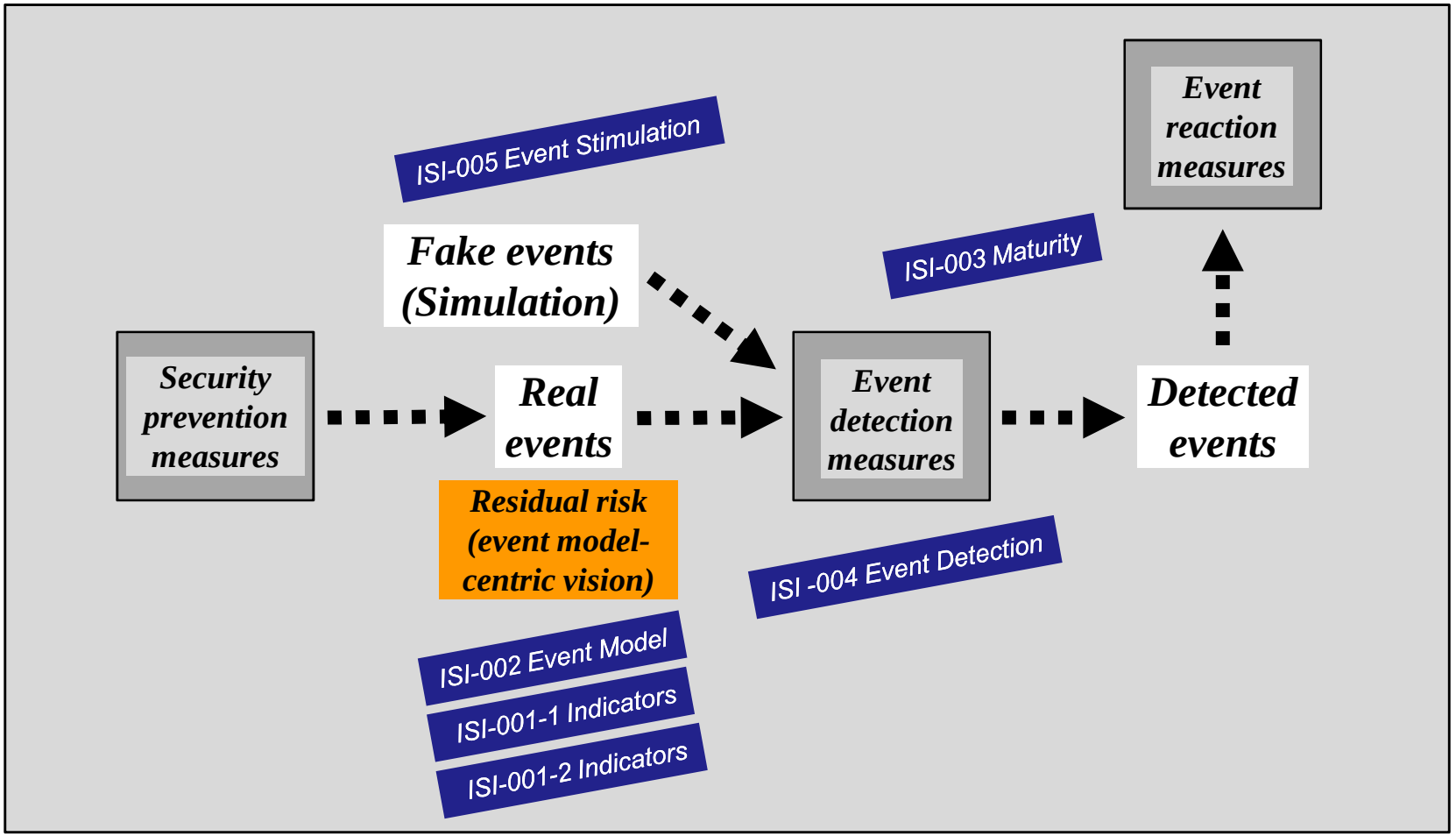


Address the scope of main missing security event detection standardization issues

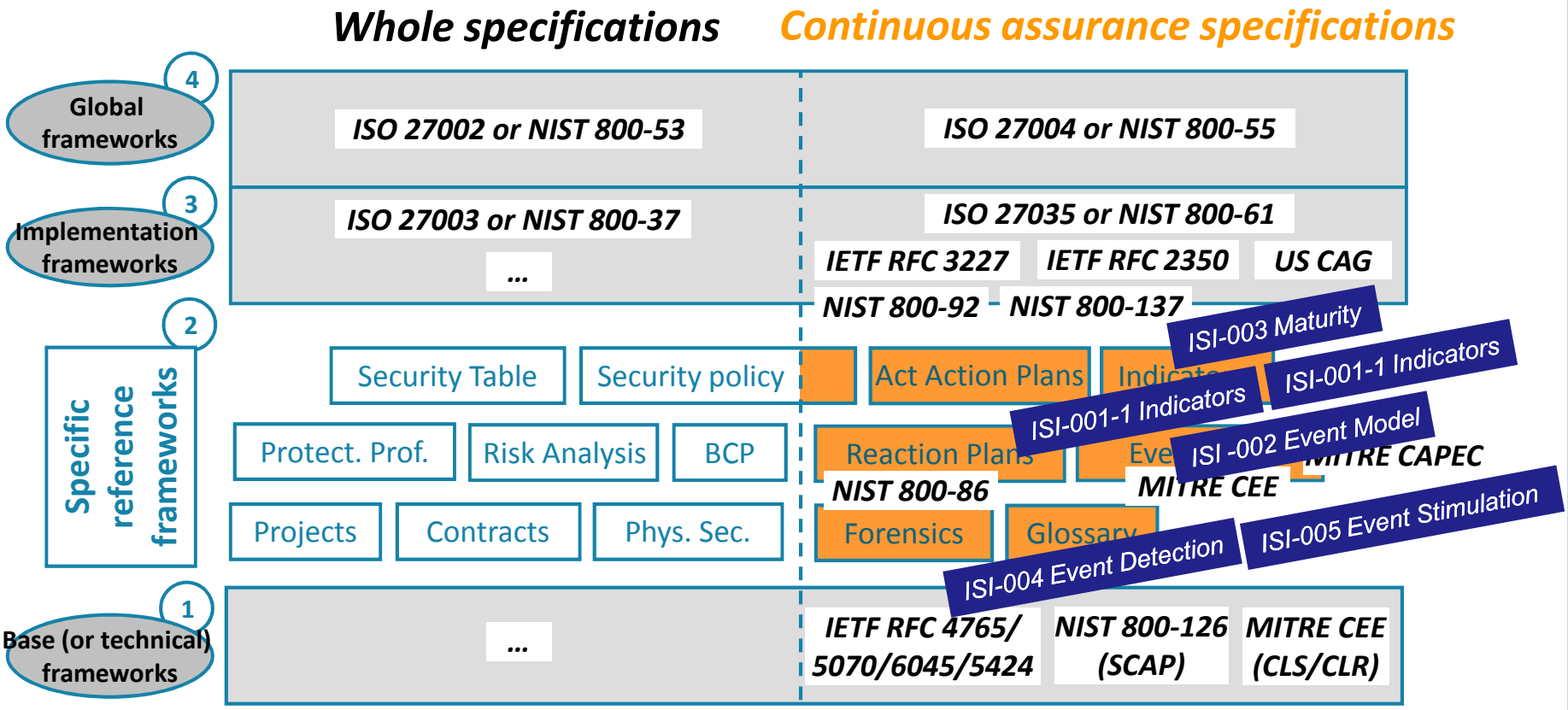
5 closely linked Work Items

- **ISI Indicators (ISI-001-1 and Guide ISI-001-2) = A powerful way to assess security controls level of enforcement and effectiveness (+ benchmarking)**
- **ISI Event Model (ISI-002) = A comprehensive security event classification model (taxonomy + representation)**
- **ISI Maturity (ISI-003) = Necessary to assess the maturity level regarding overall SIEM capabilities (technology/people/process) and to weigh event detection results. Methodology complemented by ISI-005 (which is a more detailed and case by case approach)**
- **ISI Event Detection (ISI-004) = Demonstrate through examples how to produce indicators and how to detect the related events with various means and methods (with classification of use cases/symptoms)**
- **ISI Event Stimulation (ISI-005) = Propose a way to produce security events and to test the effectiveness of existing detection means (for major types of events)**

ISI Work Items Positioning



ISI Work Items positioned against other standards



ISG ISI (Information Security Indicators)

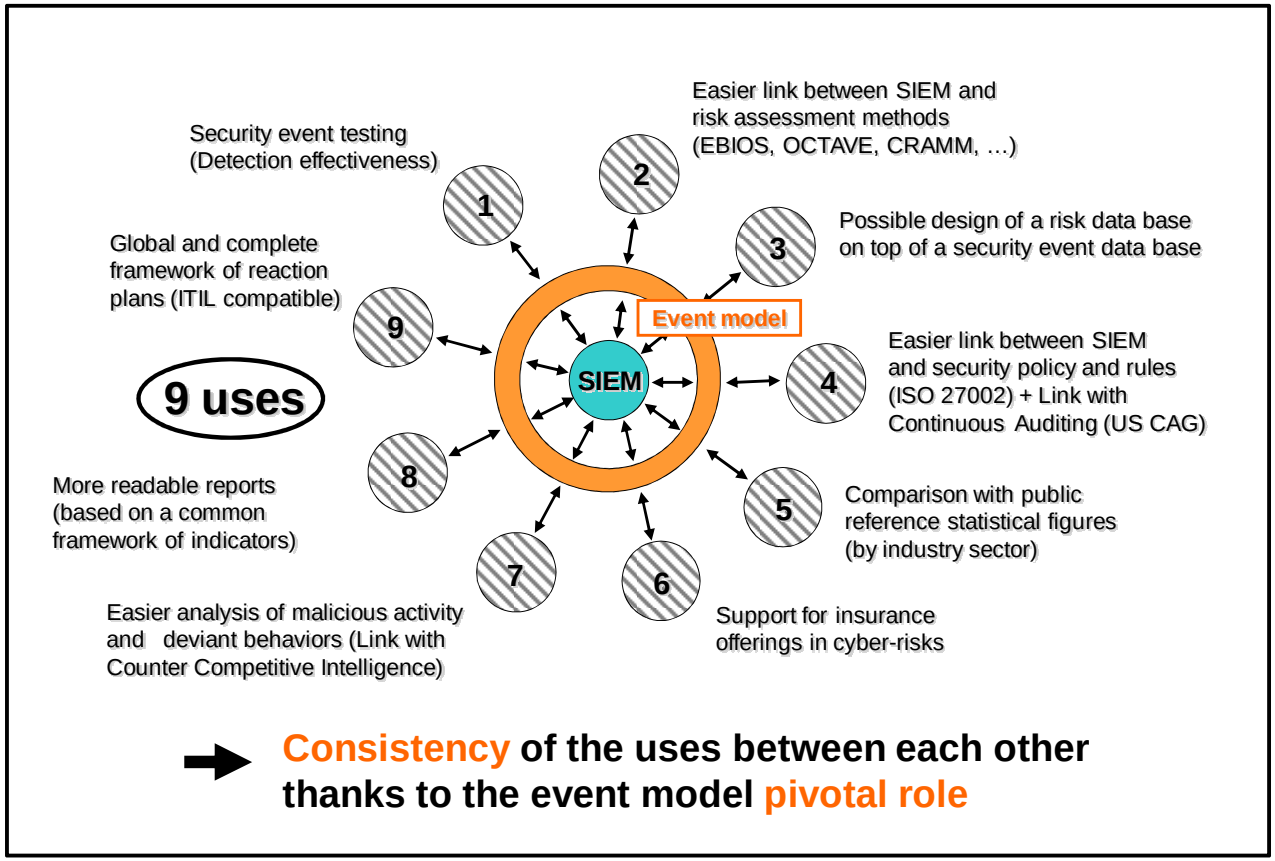
ISI-001 specifications

Position the proposed operational indicators against ISO 27002 controls and ISO 27006 technical controls = provide more assurance to governance and auditors

ISO 27002 control areas	ISO 27006 technical control areas	Incident type indicators	Vulnerability (behavioural, software, configuration, general security) type indicators	Comments
A5				Non-continuous checking
A6				Purely organisational issues
A7		IWH_UNA.1	VTC_NRG.1 VOR_PRT.1	Information classification + asset management
A8	x	IMF_LOM.1 IDB_UID.1 IDB_RGH.1 to 7 IDB_IDB.1 IDB_MIS.1 IDB_IAC.1 IDB_LOG.1	VBH_PRC.1 to 6 VBH_IAC.1 to 2 VBH_FTR.1 to 3 VBH_WTI. 1 to 6 VBH_PSW.1 to 3 VBH_RGH.1 VBH_HUW.1 to 2	Focus on deviant internal behaviours
A9	x	IEX_PHY.1	VTC_PHY.1	Marginal topic for a SIEM approach
…	…	…	…	…
A15	**XX**	IMF_TRF.2 to 3	VBH_IAC.2 VBH_WTI.2 VBH_WTI.6 VBH_RGH.1 VCF_DIS.1 VCF_TRF.1 VCF_FWR.1 VCF_ARN.1 VCF_UAC.1 to 3 VTC_IDS.1	Focus on configuration vulnerabilities or non-conformities

ISI-002 specifications (1)

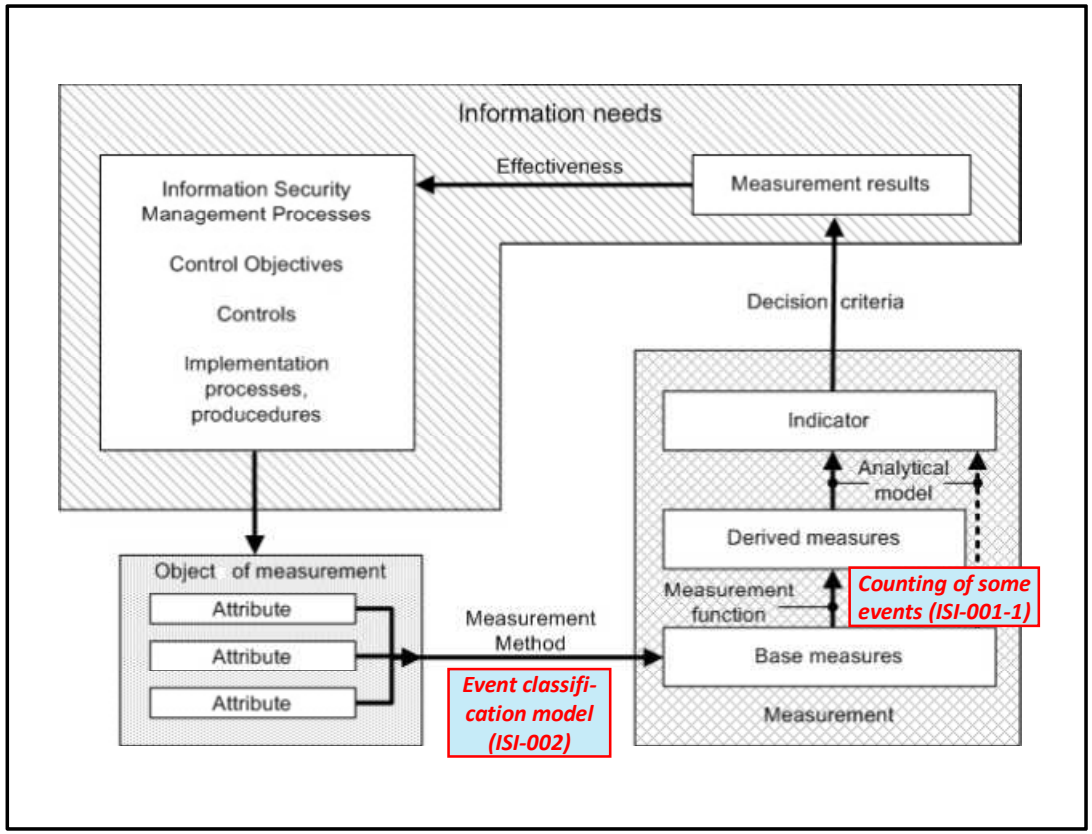
The diversified uses of the event model



Consistency of the uses between each other thanks to the event model pivotal role

ISI-002 specifications (2)

ISI-001 and ISI-002 against the ISO 27004 standard measurement model



ISI-003 specifications

The mandatory taking into account of the organization's SIEM maturity level

- A good security event detection level (still often very low today) requires many conditions (tools appropriately configured, advanced processes especially for use case creation, seasoned experts)
- This overall maturity level can be ***assessed accurately through 10 KPIs*** (with a clear correspondence with the 20 US CAG Critical Controls)
- Provision (with these KPIs) of a reckoning formula to assess its detection levels with major kinds of security events (and to weigh the results of its own measurements)
- This methodology may be complemented by a more dedicated and case by case one based on the production of security events and testing of the effectiveness of existing detection means (for major types of events)

ISI-005 specifications

Guidelines to stimulate security events are missing and are required (same motivations as ISI-003)

- Objective of testing of detection means and tools during development and deployment phases (lab and in-operation situations), and of ***measurement of their effectiveness***
- Stimulate existing detection means by relevant events (see ISI-002)
  - Try/perform fake incidents (to be identified/count)
  - Introduce vulnerabilities (to be identified/count)
- Will rest on existing test patterns (Cf. DIAMONDS project), with provision of catalogs (methods, configurations, scenarios)
- Could also be used for penetration testing
- More technical than conceptual specifications

ISG ISI schedule

Several standards just available

- **ISG ISI started in Autumn 2011 = Members of the Unit and of the 5 Work Items are European and US experts**
- **ISI Indicators (ISI-001-1 and ISI-001-2 Companion Guide) and ISI Event Model (ISI-002) are being published**
- **ISI Maturity (ISI-003) might be available by the end of 2013**
- **ISI Event Detection (ISI-004) started at the beginning of 2013**
- **ISI Event Stimulation (ISI-005) started at the beginning of 2013**