

## Regulatory Compliance Information Day

*hosted by: OMG's Regulatory Compliance Domain Special Interest Group*

## OMG Technical Meeting Special Event

Ottawa, Ontario, Canada - Wednesday, June 25, 2008

| [Agenda](#) | [Registration](#) | [All Special Events](#) | [Back to TC Meeting Info](#) | [Hotel Information](#) |

---

### Regulatory Compliance Information Day

The Regulatory Compliance Domain Special Interest Group at OMG is inviting Chief Compliance Officers, Chief Privacy Officers, Chief Security Officers, anyone who handles GRC issues for their government agency or corporation, and vendors of GRC products, to attend this Information Day. Leading experts, including regulators, vendors and consumers of GRC products will discuss the latest standardization efforts and initiatives in the GRC space. They will also describe their experiences and discuss the challenges they face, particularly in the areas of privacy, security, environmental and financial regulations from both a Canadian and international perspective. Audience participation is welcome and encouraged. Networking opportunities will be available during the scheduled breaks.

To register for this event, click [here](#).

**NOTE:** *If you register for the Technical Meeting Week, you do not have to pay the additional fee(s) to attend any or all of the special events. If you register only for special events, the special fees apply.*

#### AGENDA ( [PDF Format](#) )

- |                      |  |
|----------------------|--|
| <b>9:00 – 9:10</b>   | <b>Welcome &amp; Introduction</b><br><i>Andrew Watson, Vice President &amp; Technical Director, Object Management Group</i>              |
| <b>9:10 – 10:00</b>  | <b>Keynote Presentation</b><br><i>Dr. Mark Vale, Chief Information and Privacy Officer, Ontario</i>                                      |
| <b>10:00 – 10:20</b> | <b>GRC Roundtable and GRC-GRID Project at OMG</b><br><i>Dr. Adrian Bowles, Program Director, GRC Roundtable</i>                          |
| <b>10:20 – 10:40</b> | <b>OMG Standardization Activities Briefing</b><br><i>Andrew Watson, Vice President &amp; Technical Director, Object Management Group</i> |
| <b>10:45 – 11:00</b> | <b>Morning Refreshments</b>  |
| <b>11:00 – 11:20</b> | <b>Activities of the Regulatory Compliance DSIG</b><br><i>John Hall, Co-Chair, OMG Regulatory Compliance DSIG</i>                        |

The OMG Regulatory Compliance Domain Special Interest Group (RCDSIG) is focused on Governance, Risk and Compliance from two perspectives: · Business decisions on compliance action - see the afternoon presentation 'Management and Reaction to Regulation' ;· The possibilities for automation of compliance, starting with tools and practices currently in use. The RCDSIG works closely with the GRC Roundtable and GRC-GRID Project (see preceding presentation). Much of its work involves collaboration with task forces and other SIGs in the OMG, notably, in recent months, with the Software Assurance Architecture Board SIG - see the afternoon presentation 'The Role of Software Assurance in GRC'.

11:20 – 11:40

**The Role of SOA in Governance, Risk, and Compliance**

*Fred A. Cummins, EDS Fellow, EDS Applications Services, EDS*

SOA should be viewed as an architecture for design of the enterprise that is enabled and supported by IT. Consequently, SOA governance is enterprise governance with consideration of the impact of SOA and the optimal use of information technology. A SOA enterprise clarifies responsibilities and improves control for compliance with regulations and business policies.

11:40 – 12:00

**Certification and Accreditation: Integrating C&A into the System Lifecycle**

*Rama Moorthy, President & CEO, Hatha Systems*

Certification and Accreditation is an audit process used to evaluate and approve the security posture of systems and infrastructure prior their release to the operational environment. This audit process is used in support of organizational risk management program. Certification and Accreditation is used extensively in both government and banking sectors.

Certification and Accreditation (C&A) process has been a critical element of both systems and infrastructure component release into enterprise operational environment. Along with much of Security, C&A has also been a bolt on to the development and integration lifecycle. With new efforts to pull security earlier into the lifecycle, C&A has also moved in this direction. Ms. Moorthy will speak to various industry and government trends including the various frameworks, processes, and the legislative dicta (Sarbanes-Oxley, HIPPA, FISMA) and will address the value of the lifecycle approach.

12:00 – 14:00

**OMG Lunch & Plenary Presentations**

14:00 – 14:40

**Defense Systems and GRC**

(Demo using GRC-GRID and US DoD Standards and Regulations)

*Dr. Robert Nick Stavros, Senior Systems Engineer The MITRE Corporation*

The goal of Engineering Governance is to define a general model that describes the various aspects of governance that can be the basis of communication among governance efforts. Three aspects (Regulation, Execution and Compliance) comprise Governance. Combining these aspects with the five layers (Data, Information, Knowledge, Understanding and Wisdom) of the Cognitive Model results in 15 different governance roles. Aspect-specific Conceptual Data Models describe each of the roles. Governance objects and the relationships between the objects comprise the Conceptual Models. Finally, there are behavior rules for some of the objects.

14:40 - 15:00

**The Compliance Challenge for Global Software Vendors**

*Abdel Krim Hamou-Lhadj, Manager, Regulatory Compliance and Quality Assurance, Cognos*

For most industries in the global economy, regulations, standards and guidelines have become an integral part of the business landscape. More than ever before, regulated companies are required to abide by the regulations and diligently follow the standards and guidelines that are relevant to their industries. The process by which regulated companies do that is commonly called "Compliance Management".

What is new in the field of Compliance Management is that regulated companies have greater expectations of their software vendors to support their efforts in the compliance activities area. This puts software companies in a new situation that is completely transforming their views on how to develop software products and do business.

For global software vendors, supporting regulated customers for compliance represents a significant challenge. From the business standpoint, the challenge could become a serious burden if addressed inefficiently or a liability if not addressed at all. And from the technical standpoint, the challenge could involve addressing hundreds, or thousands, of regulations, standards and guidelines that may potentially conflict with one another.

15:00 - 15:20

**Management and Reaction to Regulation**

*John Hall & Said Tabet, Co-Chairs, OMG Regulatory Compliance DSIG*

Dealing with regulations from multiple sources is a significant burden for regulated organizations, especially small and medium-sized enterprises. Specific problems include:

- Ambiguity: the same words meaning different things in different contexts
- Overlap of, and conflicts between, different regulations
- That the effects of compliance are cumulative - new decisions have to take account of preceding decisions

The OMG Regulatory Compliance DSIG is leading development of new OMG specifications based on the recently-published 'Semantics of Business Vocabulary and Business Rules' (SBVR) and the 'Business Motivation Model'. The target domain is tools to support business people in reacting to regulation - impact analysis, risk analysis, compliance decisions and traceability from received regulation to implemented compliance action and reporting. This work is co-ordinated both with other groups in the OMG and external standards bodies.

15:20 – 15:40

**Afternoon Refreshments**

15:40 – 16:10

**Keynote Presentation: On Best Practices for Disclosure Procedures and Controls**

*Guy David, Partner, Business Law, Gowlings, Ottawa, Canada*

Guy David will be speaking on best practices for disclosure procedures and controls, regulatory issues related to disclosure of information, and potential liabilities for executives involved in disclosure of information to regulators and the public. He will be addressing this topic from a practical standpoint, both from the point of view of those involved in complying with disclosure obligations, and will also provide insight on the regulators' perspectives.

16:10 – 16:30

**Software Assurance Ecosystem: Role of Open Standards in Software Assurance as a Key Enabler for GRC**

*Djenana Campara, CEO, KDM Analytics - Co-Chair, OMG Software Assurance ABSIG*

Regulatory Compliance is a very challenging topic, particularly when it comes to balancing security and privacy requirements. SwA plays a key role in balancing and enabling GRC within software systems. As existing software systems get larger and more complex, they evolve into challenging and often conflicting designs that hinder system comprehension, compromise architectural integrity and decrease maintenance productivity. This creates severe problems moving forward. The system becomes more defect-prone, vulnerable to attacks and resistant to enhancements what in turns drastically reduces a level of confidence in security of the system. For this reason Software Assurance (SwA) community introduced SwA Ecosystem Framework that would enable industry and government to leverage and connect existing standards, policies, practices, processes and tools, in an affordable and efficient manner assisting them in building and deploying more secure products. SwA Ecosystem is based entirely on ISO/OMG Open Standards enabling integration of static and dynamic analysis tools into comprehensive SwA solution.

16:30 – 17:00

**Governance Requirements for Information Security**

*Leslie Guyatt, Project Director - Enterprise Information Security Environment, DND*

*W. Craig Campbell, Chief Security Architect, EISE Project, DND*

Over the next number of years, DND will be re-architecting its information environment: from the current amalgamation of stovepipe information systems (IS) to one that enables information centric operations; from one that relies on unstructured information, or at best semi-structured information – to a structured information environment; and from one that is primarily limited to domain specific operation to one that can seamlessly support joint, allied, inter-agency and coalition network centric operations. To accomplish this move to an Enterprise Architectural model and domain consolidation, good governance is required: consistent management, cohesive policies, processes and decision-rights for a given area of responsibility which affect the way people direct, administer or control the enterprise environment. A key factor in good governance is compliance - conforming to specifications of policy, that that has been clearly defined. This address will outline the proposed architecture governance and compliance structure for Information Management and Information Security.

17:00 - 17:15

**Questions & Answers - Wrap-Up**

18:00 - 20:00

**OMG Technical Meeting Reception**

*(all Regulatory Compliance Information Day attendees are invited)*

Edited by Kevin on June 23, 2008