The OMG GRC GRID

High Level Overview

Object Management Group GRC Program

http://www.omg.org/

QuickTime™ and a
decompressor
are needed to see this picture.

Introduction

- The Object Management Group was founded in 1989. Today, with over 470 member organizations, OMG is the largest and longest standing not-for-profit, open-membership consortium developing and maintaining computer industry specifications.
- OMG members define standards with a worldwide, neutral, open, accessible and *rapid* development process that assures *freely available specifications with implementations*
- OMG members are currently developing standards in two dozen verticals including:
  - ➢ Finance, Healthcare, Business Modeling & Integration, e-Government

OMG Specifications

MODEL DRIVEN ARCHITECTURE

UNIFIED MODELING LANGUAGE UML

CORBA

OMG Relationships

ISO

OASIS

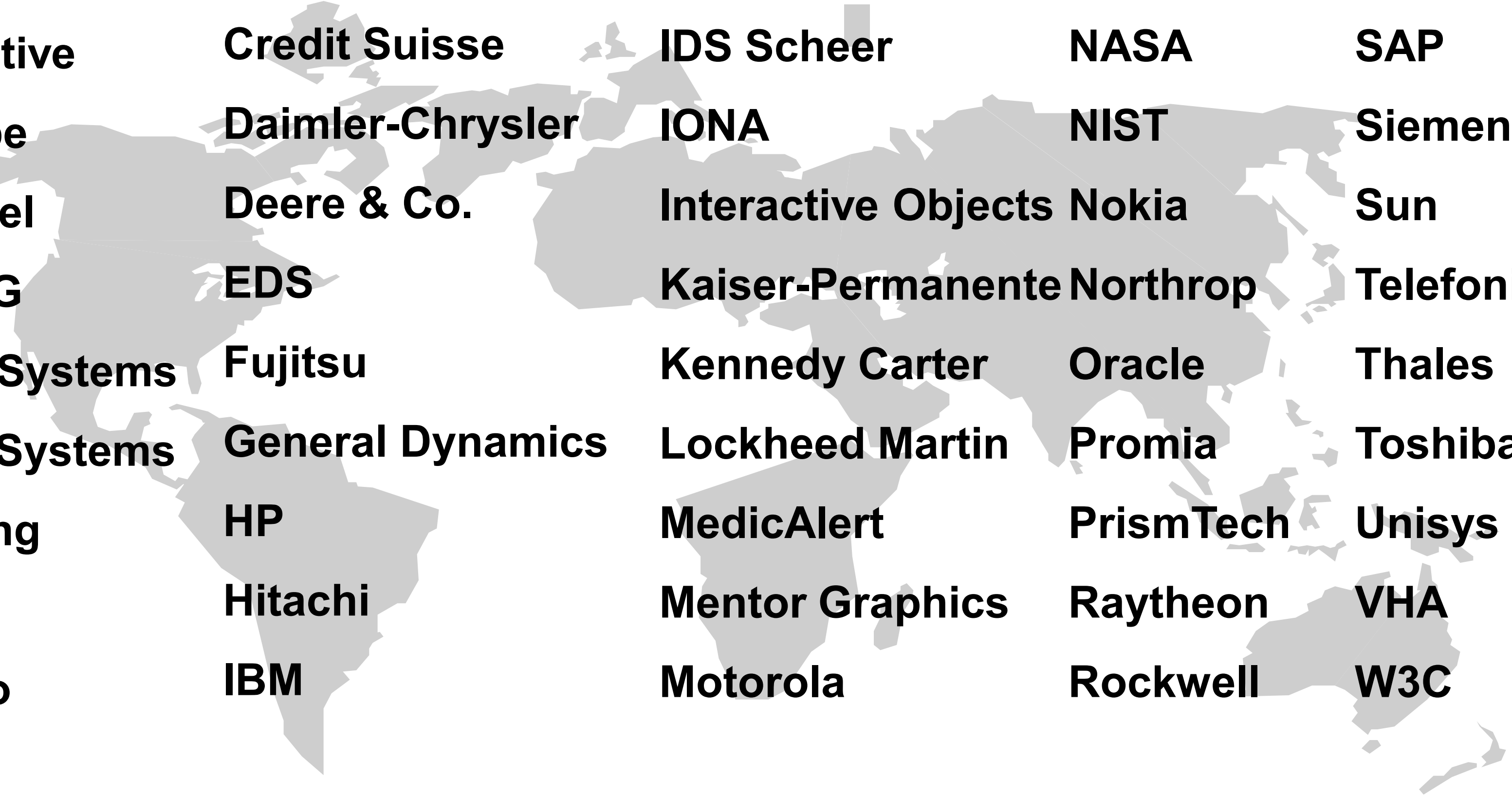
W3C WORLD WIDE WEB consortium

IEEE Networking the World

THE Open GROUP

QuickTime™ and a
decompressor
are needed to see this picture.

Who are OMG?



Adaptive
Adobe
Alcatel
ASMG
BAE Systems
BEA Systems
Boeing
CA
Cisco

Credit Suisse
Daimler-Chrysler
Deere & Co.
EDS
Fujitsu
General Dynamics
HP
Hitachi
IBM

IDS Scheer
IONA
Interactive Objects
Kaiser-Permanente
Kennedy Carter
Lockheed Martin
MedicAlert
Mentor Graphics
Motorola

NASA
NIST
Nokia
Northrop
Oracle
Promia
PrismTech
Raytheon
Rockwell

SAP
Siemens
Sun
Telefonica
Thales
Toshiba
Unisys
VHA
W3C

QuickTime™ and a
decompressor
are needed to see this picture.

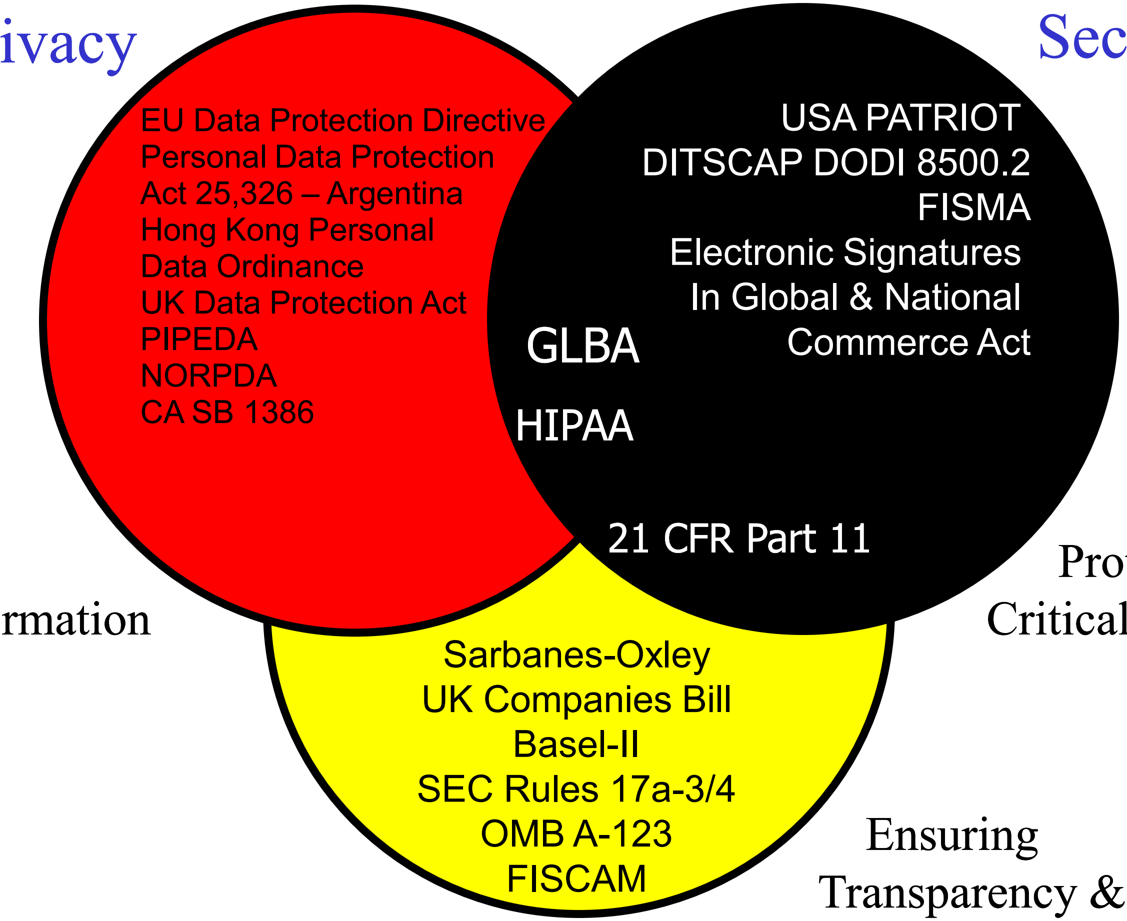
The OMG and Regulatory Compliance

- OMG Members - mostly global firms - were struggling with regulatory compliance costs and complexities
- OMG reviewed available resources, and determined that a lack of standards for modeling regulations was hindering development of better tools to automate common compliance tasks
- The OMG launched initiatives to address these issues in April 2005

Overlapping Intents & Requirements

Privacy

Security



EU Data Protection Directive
Personal Data Protection
Act 25,326 – Argentina
Hong Kong Personal
Data Ordinance
UK Data Protection Act
PIPEDA
NORPDA
CA SB 1386

USA PATRIOT
DITSCAP DODI 8500.2
FISMA
Electronic Signatures
In Global & National
Commerce Act

GLBA

HIPAA

21 CFR Part 11

Sarbanes-Oxley
UK Companies Bill
Basel-II
SEC Rules 17a-3/4
OMB A-123
FISCAM

Protecting
Private Information

Protecting
Critical Data/Infrastructure

Ensuring
Transparency & Validity

Governance

QuickTime™ and a
decompressor
are needed to see this picture.

GRC Today: Basic Findings

- Governance issues are becoming pervasive, so identifying and exploiting common enterprise and IT governance best practices will pay increasing dividends;
- Enterprise risk management is emerging as a cross-functional discipline, but progress is hampered by the lack of relevant standards and interoperable tools;
- Regulatory compliance costs IT departments billions of dollars annually
- Rules are often complex, occasionally in conflict with each other, and always subject to change.
- Competitors within a market typically gain no sustainable advantage through their GRC investments, but divert capital and management resources that could be used to grow their enterprises.
- Failures can cause cascading loss of confidence within a market, so it is to every participant's advantage to collaborate and share these practices.
- GRC tools should interoperate seamlessly using open specifications for GRC data representation.

QuickTime™ and a
decompressor
are needed to see this picture.

The Problem

- Growing number of International, National and Local regulations, standards, policies
- Growing number of conflicts, redundancies, overlaps
- Multiple jurisdictions, conflicts in areas of privacy and security, reporting, etc
- Where does one find guidance on: which ones apply in Canada? When do they apply? What is the impact to a specific sector of the economy? Implementation options?

The OMG GRID helps address these questions

QuickTime™ and a decompressor are needed to see this picture.

The GRID: Goals and Objectives

- Provide the regulatory agencies to provide and publish guidance on the application of specific and interrelated regulations

- Improve the ability of **enterprises** and **government agencies** to:
  - Effectively comply and demonstrate compliance with relevant regulations
  - Reduce the time, and initial and on-going costs of complying with regulations

- Improve the ability of **vendors** of IT based products and services to develop offerings that:
  - comply with regulations, or that
  - enable the planning, implementation and control of processes and rules to comply with regulations

QuickTime™ and a
decompressor
are needed to see this picture.

GRC- GRID Geography Scope

The first release of the GRID is focused on the banking vertical, and includes rules from the following countries:

Argentina
Australia
Belgium
Brazil
Canada
China
France
Germany

Hong Kong
India
Italy
Japan
Luxembourg
Mexico
Netherlands
Portugal

Singapore
South Korea
Spain
Sweden
Switzerland
United Kingdom
USA

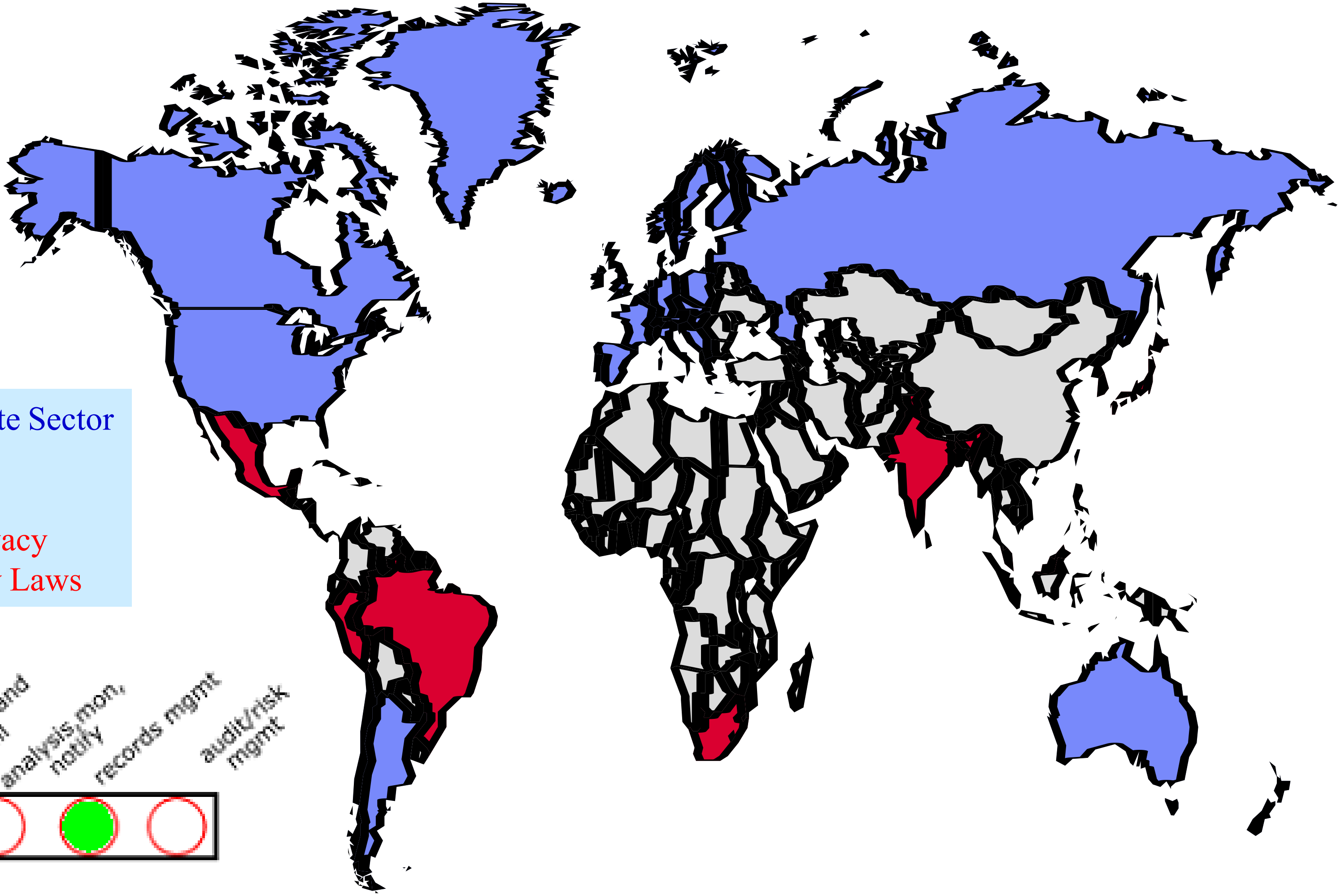
and multi-national entities such as the European Union (EU)

QuickTime™ and a
decompressor
are needed to see this picture.

Types of Rules Captured

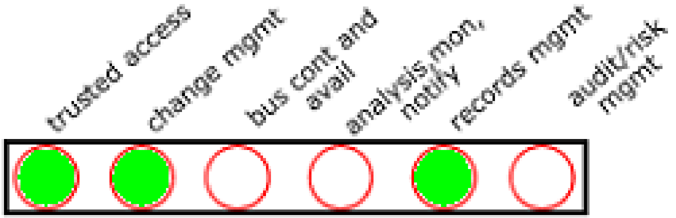
- Outsourcing Regulations / Principles / Guidelines
- IT Governance and Operational Risk (incl. IT risk) Management
- Data Privacy & Transfer
- Spam
- Data Retention & Secrecy
- Security & Safety of IT Systems and Infrastructure
- Business Resiliency (incl. BCP/DRP)
- Electronic Surveillance & Monitoring
- Electronic Transactions & Digital Signatures
- Networks & Firewall Policies.

Global snapshot on privacy laws



Blue--Existing Private Sector Privacy Laws

Red---Emerging privacy Sector Privacy Laws



QuickTime™ and a decompressor are needed to see this picture.

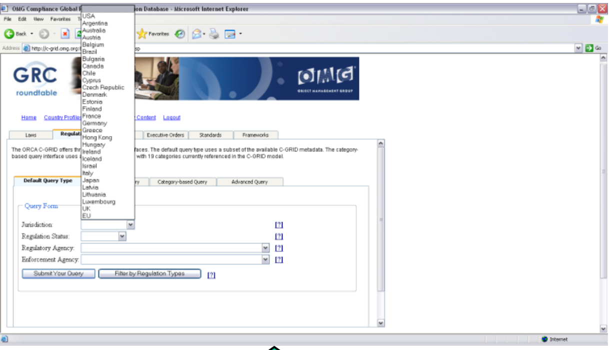
Privacy in Canada

- CAN SPAM Act
- Canadian Comprehensive Auditing Foundation
- Canadian Public Accountability Board (CPAB)
- Canadian Securities Administrators (CSA) Proposed Multilateral Instrument 52-111
- CanCERT
- DRIE Canada (Disaster Recovery Information Exchange)
- Institute of Chartered Accountants of Ontario
- Multilateral Instrument 52-109 - Ontario Securities Commission
- Multilateral Instrument 52-110: Audit Committees
- PIPEDA (CAN/CSA-Q830-96)

QuickTime™ and a decompressor are needed to see this picture.

Integrating the GRID with a Policy Management Platform

- Linking Regulatory Requirements to Internal Policy
- Enable the company/Client to comply with regulatory requirements
- Provide traceability and transparency
- Continuous Audit-ability: assess the effectiveness of policies and mitigate risks



OMG Compliance Global R… on Database - Microsoft Internet Explorer

Address http://c-grid.omg.org/…sp

The ORCA C-GRID offers thr… …faces. The default query type uses a subset of the available C-GRID metadata. The category-based query interface uses … with 19 categories currently referenced in the C-GRID model.

Query Form

Jurisdiction: [?]

USA
Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hong Kong
Hungary
Ireland
Iceland
Israel
Italy
Japan
Latvia
Lithuania
Luxembourg
UK
EU

Regulation Status: [?]

Regulatory Agency: [?]

Enforcement Agency: [?]

Submit Your Query | Filter by Regulation Types [?]

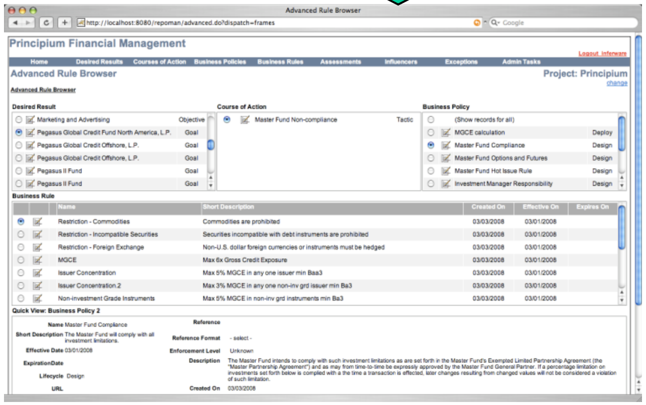
Policies, Corporate Actions,

Assessments, Rules, Processes

Regulations

Frameworks

Guidelines,…



Advanced Rule Browser

http://localhost:8080/repoman/advanced.do?dispatch=frames

Principium Financial Management

Advanced Rule Browser — Project: Principium

Advanced Rule Browser

Desired Result

○	Marketing and Advertising	Objective
●	Pegasus Global Credit Fund North America, L.P.	Goal
○	Pegasus Global Credit Offshore, L.P.	Goal
○	Pegasus Global Credit Offshore, L.P.	Goal
○	Pegasus II Fund	Goal
○	Pegasus II Fund	Goal

Course of Action

●	Master Fund Non-compliance	Tactic

Business Policy

○	(Show records for all)	
○	MGCE calculation	Deploy
●	Master Fund Compliance	Design
○	Master Fund Options and Futures	Design
○	Master Fund Hot Issue Rule	Design
○	Investment Manager Responsibility	Design

Business Rule

	Name	Short Description	Created On	Effective On	Expires On
●	Restriction - Commodities	Commodities are prohibited	03/03/2008	03/01/2008	
○	Restriction - Incompatible Securities	Securities incompatible with debt instruments are prohibited	03/03/2008	03/01/2008	
○	Restriction - Foreign Exchange	Non-U.S. dollar foreign currencies or instruments must be hedged	03/03/2008	03/01/2008	
○	MGCE	Max 6x Gross Credit Exposure	03/03/2008	03/01/2008	
○	Issuer Concentration	Max 5% MGCE in any one issuer min Baa3	03/03/2008	03/01/2008	
○	Issuer Concentration 2	Max 3% MGCE in any one non-inv grd issuer min Ba3	03/03/2008	03/01/2008	
○	Non-investment Grade Instruments	Max 5% MGCE in non-inv grd instruments min Ba3	03/03/2008	03/01/2008	

Quick View: Business Policy 2

Name Master Fund Compliance

Short Description The Master Fund will comply with all investment limitations.

Effective Date 03/01/2008

ExpirationDate

Lifecycle Design

URL

Reference

Reference Format - select -

Enforcement Level Unknown

Description The Master Fund intends to comply with such investment limitations as are set forth in the Master Fund's Exempted Limited Partnership Agreement (the "Master Partnership Agreement") and as may from time-to-time be expressly approved by the Master Fund General Partner. If a percentage limitation on investments set forth below is complied with a the time a transaction is effected, later changes resulting from changed values will not be considered a violation of such limitation.

Created On 03/03/2008

QuickTime™ and a decompressor are needed to see this picture.

What do you get out of the Box

- The GRID Framework (can be customized or ready to use as is)
- A starter kit containing a few hundred regulations, guidelines and related industry frameworks
- A strong model based on formal methodology and standards
- A related vocabulary of terms for all Canadian Jurisdiction in one vertical Additional jurisdiction and vertical can be added as part of the customization
- An integration Kit to enable the use of GRID in Web-based distributed environments

QuickTime™ and a
decompressor
are needed to see this picture.

What do you get to develop

- Extending the GRID to fit your specific requirements
- A taxonomy to classify your regulatory and risk view (supported by the GRID framework)
- Vocabularies, interpretations of relevant regulations to store in the GRID repository

QuickTime™ and a
decompressor
are needed to see this picture.

What are the related costs?

- Initial Costs
  - Sponsoring and Licensing for the GRID: USD 200k annually
  - Maintenance: free 1st year then 15% a year
    (includes all GRID upgrades)
  - Hosting: USD 5k per month

- Estimated Implementation Costs
  - Custimization: USD 25k per month for three months minimum
  - Assuming internal resources available on a part time basis

QuickTime™ and a
decompressor
are needed to see this picture.

Thank You!

For any questions, please contact:
ken@omg.org

QuickTime™ and a
decompressor
are needed to see this picture.