Object Management Group

109 Highland Avenue
Needham, MA 02494
USA

Telephone: +1-781-444-0404
Facsimile: +1-781-444-0320
rfp@omg.org

UML Operational Threat & Risk Model Request for Proposal

OMG Document: SysA/2014-06-17

Letters of Intent due: January 5th 2015
Submissions due: February 23rd, 2015

Objective of this RFP

In the broadest sense, organizations manage threats and risks in order to provide a systematic response to uncertainties and enhance situational awareness. Multiple communities have developed data and exchange schema and interfaces for sharing information about threats, risks and incidents that impact important government, commercial and personal assets and privacy. While each of these schema and interfaces provides value for a specific community it is difficult to federate these multiple representations to arrive at broad-based planning, simulation, assessment, situational awareness and forensics, and to then enact the appropriate courses of action. Cyber related attacks have added a new dimension that stresses traditional assessment, monitoring and mitigation strategies.

This RFP calls for a conceptual model for operational threats and risks that unifies the semantics of and can provide a bridge across multiple threat and risk schema and interfaces. The conceptual model will be informed by high-level concepts as defined by the Cyber domain, existing NIEM domains and other applicable domains, but is not specific to those domains. This will enable combined Cyber, physical, criminal and natural threats and risks to be federated, understood and responded to effectively.

Out of scope for this RFP is non-operational business relevant risk such as marketplace risk, credit risk, legal risk, project management risk, etc.

The conceptual model will have an information exchange format based on NIEM[1] and an explicit mapping to STIX[2]. Other exchange formats, such as CAP[3] may be supported as well.

For further details see Section 6 of this document.

1 Introduction

1.1 Goals of OMG

The Object Management Group (OMG) is a software consortium with an international membership of vendors, developers, and end users. Established in 1989, its mission is to help computer users solve enterprise integration problems by supplying open, vendor-neutral portability, interoperability and reusability specifications based on Model Driven Architecture (MDA). MDA defines an approach to IT system specification that separates the specification of system functionality from the specification of the implementation of that functionality on a specific technology platform, and provides a set of guidelines for structuring specifications expressed as models. OMG has published many widely-used specifications such as UML [UML], BPMN [BPMN], MOF [MOF], XMI [XMI], DDS [DDS] and CORBA [CORBA], to name but a few significant ones.

1.2 Organization of this document

The remainder of this document is organized as follows:

Section 2 – Architectural Context. Background information on OMG's Model Driven Architecture.

Section 3 – Adoption Process. Background information on the OMG specification adoption process.

Section 4 – Instructions for Submitters. Explanation of how to make a submission to this RFP.

Section 5 – General Requirements on Proposals. Requirements and evaluation criteria that apply to all proposals submitted to OMG.

---

[1]NIEM: National Information Exchange Model (www.niem.gov)

[2] STIX: (Structured Threat Information Expression): http://stix.mitre.org

[3] CAP: http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html

Section 6 – Specific Requirements on Proposals. Problem statement, scope of proposals sought, mandatory requirements, non-mandatory features, issues to be discussed, evaluation criteria, and timetable that apply specifically to this RFP.

Appendix A – References and Glossary Specific to this RFP

Appendix B – General References and Glossary

1.3 Conventions

The key words "shall", "shall not", "should", "should not", "may" and "need not" in this document should be interpreted as described in Part 2 of the ISO/IEC Directives [ISO2]. These ISO terms are compatible with the same terms in IETF RFC 2119 [RFC2119].

1.4 Contact Information

Questions related to OMG's technology adoption process and any questions about this RFP should be directed to rfp@omg.org.

OMG documents and information about the OMG in general can be obtained from the OMG's web site: http://www.omg.org. Templates for RFPs (like this document) and other standard OMG documents can be found on the Template Downloads Page: http://www.omg.org/technology/template_download.htm

2 Architectural Context

MDA provides a set of guidelines for structuring specifications expressed as models and the mappings between those models. The MDA initiative and the standards that support it allow the same model, specifying business system or application functionality and behavior, to be realized on multiple platforms. MDA enables different applications to be integrated by explicitly relating their models; this facilitates integration and interoperability, and supports system evolution (deployment choices) as platform technologies change. The three primary goals of MDA are portability, interoperability and reusability.

Portability of any subsystem is relative to the subsystems on which it depends. The collection of subsystems that a given subsystem depends upon is often loosely called the platform, which supports that subsystem. Portability – and reusability – of such a subsystem is enabled if all the subsystems that it depends upon use standardized interfaces (APIs) and usage patterns.

MDA provides a pattern comprising a portable subsystem that is able to use any one of multiple specific implementations of a platform. This pattern is repeatedly usable in the specification of systems. The five important concepts related to this pattern are:

1. **Model** – A model is a representation of a part of the function, structure and/or behavior of an application or system. A representation is said to be formal when it is based on a language that has a well-defined form ("syntax"), meaning ("semantics"), and possibly rules of analysis, inference, or proof for its constructs. The syntax may be graphical or textual. The semantics might be defined, more or less formally, in terms of things observed in the world being described (e.g. message sends and replies, object states and state changes, etc.), or by translating higher-level language constructs into other constructs that have a well-defined meaning. The (non-mandatory) rules of inference define what unstated properties can be deduced from explicit statements in the model. In MDA, a representation that is not formal in this sense is not a model. Thus, a diagram with boxes and lines and arrows that is not supported by a definition of the meaning of a box, and the meaning of a line and of an arrow is not a model – it is just an informal diagram.
2. **Platform** – A set of subsystems/technologies that provide a coherent set of functionality through interfaces and specified usage patterns that any subsystem that depends on the platform can use without concern for the details of how the functionality provided by the platform is implemented.
3. **Platform Independent Model (PIM)** – A model of a subsystem that contains no information specific to the platform, or the technology that is used to realize it.
4. **Platform Specific Model (PSM)** – A model of a subsystem that includes information about the specific technology that is used in the realization of that subsystem on a specific platform, and hence possibly contains elements that are specific to the platform.
5. **Mapping** – Specification of a mechanism for transforming the elements of a model conforming to a particular metamodel into elements of another model that conforms to another (possibly the same) metamodel. A mapping may be expressed as associations, constraints, rules or templates with parameters that to be assigned during the mapping or other forms yet to be determined.

OMG adopts standard specifications of models that exploit the MDA pattern to facilitate portability, interoperability and reusability, either through ab initio development of standards or by reference to existing standards. Some examples of OMG adopted specifications are:

- Languages – e.g. IDL for interface specification [IDL], UML for model specification [UML], BPMN for Business Process specification [BPMN], etc.

6. Mappings – e.g. mapping of OMG IDL to specific implementation languages (CORBA PIM to Implementation Language PSMs), UML Profile

for EDOC (PIM) to CCM (CORBA PSM) and EJB (Java PSM), and CORBA (PSM) to COM (PSM) etc.

7. Services – e.g. Naming Service [NS], Transaction Service [OTS], Security Service [SEC], Trading Object Service [TOS] etc.
8. Platforms – e.g. CORBA [CORBA], DDS [DDS]
9. Protocols – e.g. GIOP/IIOP [CORBA] (both structure and exchange protocol), DDS Interoperability Protocol [DDSI].
10. Domain Specific Standards – e.g. Model for Performance-Driven Government [MPG], Single Nucleotide Polymorphisms specification [SNP], TACSIT Controller Interface specification [TACSIT].

For an introduction to MDA, see [MDAa]. For a discourse on the details of MDA please refer to [MDAc]. To see an example of the application of MDA see [MDAb]. For general information on MDA, see [MDAd].

Object Management Architecture (OMA) is a distributed object computing platform architecture within MDA that is related to ISO's Reference Model of Open Distributed Processing RM-ODP [RM-ODP]. CORBA and any extensions to it are based on OMA. For information on OMA see [OMA].

3 Adoption Process

3.1 Introduction

OMG decides which specifications to adopt via votes of its Membership. The specifications selected should satisfy the architectural vision of MDA. OMG bases its decisions on both business and technical considerations. Once a specification is adopted by OMG, it is made available for use by both OMG members and non-members alike, at no charge.

This section 3 provides an extended summary of the RFP process. For more detailed information, see the Policies and Procedures of the OMG Technical Process [P&P], specifically Section 4.2, and the OMG Hitchhiker's Guide [Guide]. In case of any inconsistency between this document or the Hitchhiker's Guide and the Policies and Procedures, the P&P is always authoritative. All IPR-related matters are governed by OMG's Intellectual Property Rights Policy [IPR].

3.2 The Adoption Process in detail

3.2.1 Development and Issuance of RFP

RFPs, such as this one, are drafted by OMG Members who are interested in the adoption of an OMG specification in a particular area. The draft RFP is presented to the appropriate TF, discussed and refined, and when ready is

recommended for issuance. If endorsed by the Architecture Board, the RFP may then be issued as an OMG RFP by a TC vote.

Under the terms of OMG's Intellectual Property Rights Policy [IPR], every RFP shall include a statement of the IPR Mode under which any resulting specification will be published. To achieve this, RFP authors choose one of the three allowable IPR modes specified in [IPR] and include it in the RFP – see section 6.10.

3.2.2 Letter of Intent (LOI)

Each OMG Member organization that intends to make a Submission in response to any RFP (including this one) shall submit a Letter of Intent (LOI) signed by an officer on or before the deadline specified in the RFP's timetable (see section 6.11). The LOI provides public notice that the organization may make a submission, but does not oblige it to do so.

3.2.3 Voter Registration

Any interested OMG Members, other than Trial, Press and Analyst members, may participate in Task Force voting related to this RFP. If the RFP timetable includes a date for closing the voting list (see section 6.11), or if the Task Force separately decides to close the voting list, then only OMG Member that have registered by the given date and those that have made an Initial Submission may vote on Task Force motions related to this RFP.

Member organizations that have submitted an LOI are automatically registered to vote in the Task Force. Technical Committee votes are not affected by the Task Force voting list – all Contributing and Domain Members are eligible to vote in DTC polls relating to DTC RFPs, and all Contributing and Platform Members are eligible to vote in PTC polls on PTC RFPs.

3.2.4 Initial Submissions

Initial Submissions shall be made electronically on or before the Initial Submission deadline, which is specified in the RFP timetable (see section 6.11), or may later be adjusted by the Task Force. Submissions shall use the OMG specification template [TMPL], with the structure set out in section 4.9. Initial Submissions shall be written specifications capable of full evaluation and not just a summary or outline. Submitters normally present their proposals to the Task Force at the first TF meeting after the submission deadline. Making a submission incurs obligations under OMG's IPR policy – see [IPR] for details.

An Initial Submission shall not be altered once the Initial Submission deadline has passed. The Task Force may choose to recommend an Initial Submission, unchanged, for adoption by OMG; however, instead Task Force members usually offer comments and feedback on the Initial Submissions, which submitters can address (if they choose) by making a later Revised Submission.

The goals of the Task Force's Submission evaluation are:

- Provide a fair and open process
- Facilitate critical review of the submissions by OMG Members
- Provide feedback to submitters enabling them to address concerns in their revised submissions
- Build consensus on acceptable solutions
- Enable voting members to make an informed selection decision

Submitters are expected to actively contribute to the evaluation process.

3.2.5 Revised Submissions

Revised Submissions are due by the specified deadline. Revised Submissions cannot be altered once their submission deadline has passed. Submitters again normally present their proposals at the next meeting of the TF after the deadline. If necessary, the Task Force may set a succession of Revised Submission deadlines. Submitters choose whether or not to make Revised Submissions - if they decide not to, their most recent Submission is carried forward, unless the Submitter explicitly withdraws from the RFP process.

The evaluation of Revised Submissions has the same goals listed above.

3.2.6 Selection Votes

When the Task Force's voters believe that they sufficiently understand the relative merits of the available Submissions, a vote is taken to recommend a submission to the Task Force's parent Technical Committee. The Architecture Board reviews the recommended Submission for MDA compliance and technical merit. Once the AB has endorsed it, members of the relevant TC vote on the recommended Submission by email. Successful completion of this vote moves the recommendation to OMG's Board of Directors (BoD).

3.2.7 Business Committee Questionnaire

Before the BoD makes its final decision on turning a Technical Committee recommendation into an OMG published specification, it asks its Business Committee to evaluate whether implementations of the specification will be publicly available. To do this, the Business Committee will send a Questionnaire [BCQ] to every OMG Member listed as a Submitter on the recommended Submission. Members that are not Submitters can also complete a Business Committee Questionnaire for the Submission if they choose.

If no organization commits to make use of the specification, then the BoD will typically not act on the recommendation to adopt it – so it is very important that submitters respond to the BCQ.

Once the Business Committee has received satisfactory BCQ responses, the Board takes the final publication vote. A Submission that has been adopted by the Board is termed an Alpha Specification.

At this point the RFP process is complete.

3.2.8 Finalization & Revision

Any specification adopted by OMG by any mechanism, whether RFP or otherwise, is subject to Finalization. A Finalization Task Force (FTF) is chartered by the TC that recommended the Specification; its task is to correct any problems reported by early users of the published specification. The FTF first collaborates with OMG's Technical Editor to prepare a cleaned-up version of the Alpha Specification with submission-specific material removed. This is the Beta1 specification, and is made publicly available via OMG's web site. The FTF then works through the list of bug reports ("issues") reported by users of the Beta1 specification, to produce a Finalization Report and another Beta specification (usually Beta2), which is a candidate for Formal publication. Once endorsed by the AB and adopted by the relevant TC and BoD, this is published as the final, Formal Specification.

Long-term maintenance of OMG specifications is handled by a sequence of Revision Task Forces (RTFs), each one chartered to rectify any residual problems in the most-recently published specification version. For full details, see P&P section 4.4 [P&P].

4 Instructions for Submitters

4.1 OMG Membership

To submit to an RFP issued by the Platform Technology Committee an organization shall maintain either Platform or Contributing OMG Membership from the date of the initial submission deadline, while to submit to a Domain RFP an organization shall maintain either a Contributing or Domain membership.

4.2 Intellectual Property Rights

By making a Submission, an organization is deemed to have granted to OMG a perpetual, nonexclusive, irrevocable, royalty-free, paid up, worldwide license to copy and distribute the document and to modify the document and distribute copies of the modified version, and to allow others to do the same. Submitter(s) shall be the copyright owners of the text they submit, or have sufficient copyright and patent rights from the copyright owners to make the Submission under the terms of OMG's IPR Policy. Each Submitter shall disclose the identities of all copyright owners in its Submission.

Each OMG Member that makes a written Submission in response to this RFP shall identify patents containing Essential Claims that it believes will be infringed if that Submission is included in an OMG Formal Specification and implemented.

By making a written Submission to this RFP, an OMG Member also agrees to comply with the Patent Licensing terms set out in section 6.10.

This section 4.2 is neither a complete nor an authoritative statement of a submitter's IPR obligations – see [IPR] for the governing document for all OMG's IPR policies.

4.3 Submission Effort

An RFP submission may require significant effort in terms of document preparation, presentations to the issuing TF, and participation in the TF evaluation process. OMG is unable to reimburse submitters for any costs in conjunction with their submissions to this RFP.

4.4 Letter of Intent

Every organization intending to make a Submission against this RFP shall submit a Letter of Intent (LOI) signed by an officer on or before the deadline listed in section 6.11, or as later varied by the issuing Task Force.

The LOI should designate a single contact point within the submitting organization for receipt of all subsequent information regarding this RFP and the submission. The name of this contact will be made available to all OMG members. LOIs shall be sent by email, fax or paper mail to the "RFP Submissions Desk" at the OMG address shown on the first page of this RFP.

A suggested template for the Letter of Intent is available at http://doc.omg.org/loi [LOI].

4.5 Business Committee terms

This section contains the text of the Business Committee RFP attachment concerning commercial availability requirements placed on submissions. This attachment is available separately as OMG document omg/12-12-03.

4.5.1 Introduction

OMG wishes to encourage rapid commercial adoption of the specifications it publishes. To this end, there must be neither technical, legal nor commercial obstacles to their implementation. Freedom from the first is largely judged through technical review by the relevant OMG Technology Committees; the second two are the responsibility of the OMG Business Committee. The BC also looks for evidence of a commitment by a submitter to the commercial success of products based on the submission.

4.5.2 Business Committee evaluation criteria

4.5.2.1 Viable to implement across platforms

While it is understood that final candidate OMG submissions often combine technologies before they have all been implemented in one system, the Business Committee nevertheless wishes to see evidence that each major feature has been implemented, preferably more than once, and by separate organizations. Pre-product implementations are acceptable. Since use of OMG specifications should not be dependent on any one platform, cross-platform availability and interoperability of implementations should be also be demonstrated.

4.5.2.2 Commercial availability

In addition to demonstrating the existence of implementations of the specification, the submitter must also show that products based on the specification are commercially available, or will be within 12 months of the date when the specification was recommended for adoption by the appropriate Task Force. Proof of intent to ship product within 12 months might include:

- A public product announcement with a shipping date within the time limit.
- Demonstration of a prototype implementation and accompanying draft user documentation.

Alternatively, and at the Business Committee's discretion, submissions may be adopted where the submitter is not a commercial software provider, and therefore will not make implementations commercially available. However, in this case the BC will require concrete evidence of two or more independent implementations of the specification being used by end-user organizations as part of their businesses.

Regardless of which requirement is in use, the submitter must inform the OMG of completion of the implementations when commercially available.

4.5.2.3 Access to Intellectual Property Rights

OMG will not adopt a specification if OMG is aware of any submitter, member or third party which holds a patent, copyright or other intellectual property right (collectively referred to in this policy statement as "IPR") which might be infringed by implementation or recommendation of such specification, unless OMG believes that such IPR owner will grant an appropriate license to organizations (whether OMG members or not) which wish to make use of the specification. It is the goal of the OMG to make all of its technology available with as few impediments and disincentives to adoption as possible, and therefore OMG strongly encourages the submission of technology as to which royalty-free licenses will be available.

The governing document for all intellectual property rights ("IPR") policies of Object Management Group is the Intellectual Property Rights statement, available at: http://doc.omg.org/ipr. It should be consulted for the authoritative statement of the submitter's patent disclosure and licensing obligations.

4.5.2.4 Publication of the specification

Should the submission be adopted, the submitter must grant OMG (and its sub licensees) a worldwide, royalty-free license to edit, store, duplicate and distribute both the specification and works derived from it (such as revisions and teaching materials). This requirement applies only to the written specification, not to any implementation of it. Please consult the Intellectual Property Rights statement (http://doc.omg.org/ipr) for the authoritative statement of the submitter's copyright licensing obligations.

4.5.2.5 Continuing support

The submitter must show a commitment to continue supporting the technology underlying the specification after OMG adoption, for instance by showing the BC development plans for future revisions, enhancement or maintenance.

4.6 Responding to RFP items

4.6.1 Complete proposals

Submissions should propose full specifications for all of the relevant requirements detailed in Section 6 of this RFP. Submissions that do not present complete proposals may be at a disadvantage.

Submitters are encouraged to include any non-mandatory features listed in Section 6.

4.6.2 Additional specifications

Submissions may include additional specifications for items not covered by the RFP and which they believe to be necessary. Information on these additional items should be clearly distinguished. Submitters shall give a detailed rationale for why any such additional specifications should also be considered for adoption. Submitters should note that a TF is unlikely to consider additional items that are already on the roadmap of an OMG TF, since this would pre-empt the normal adoption process.

4.6.3 Alternative approaches

Submitters may provide alternative RFP item definitions, categorizations, and groupings so long as the rationale for doing so is clearly stated. Equally, submitters may provide alternative models for how items are provided if there are compelling technological reasons for a different approach.

4.7 Confidential and Proprietary Information

The OMG specification adoption process is an open process. Responses to this RFP become public documents of the OMG and are available to members and non-members alike for perusal. No confidential or proprietary information of any kind will be accepted in a submission to this RFP.

4.8 Proof of Concept

Submissions shall include a “proof of concept” statement, explaining how the submitted specifications have been demonstrated to be technically viable. The technical viability has to do with the state of development and maturity of the technology on which a submission is based. This is not the same as commercial availability. Proof of concept statements can contain any information deemed relevant by the submitter; for example:

> “This specification has completed the design phase and is in the process of being prototyped.”
>
> “An implementation of this specification has been in beta-test for 4 months.”
>
> “A named product (with a specified customer base) is a realization of this specification.”

It is incumbent upon submitters to demonstrate the technical viability of their proposal to the satisfaction of the TF managing the evaluation process. OMG will favor proposals based on technology for which sufficient relevant experience has been gained.

4.9 Submission Format

4.9.1 General

- Submissions that are concise and easy to read will inevitably receive more consideration.
- Submitted documentation should be confined to that directly relevant to the items requested in the RFP.
- To the greatest extent possible, the submission should follow the document structure set out in "ISO/IEC Directives, Part 2 – Rules for the structure and drafting of International Standards" [ISO2]. An OMG specification template is available to make it easier to follow these guidelines.
- The key words "shall", "shall not", "should", "should not", "may" and "need not" shall be used as described in Part 2 of the ISO/IEC Directives [ISO2]. These ISO terms are compatible with the same terms in IETF RFC 2119 [RFC2119]. However, the RFC 2119 terms "must", "must not", "optional", "required", "recommended" and "not recommended" shall not be used (even though they are permitted under RFC2119).

4.9.2 Mandatory Outline

All submissions shall use the following structure, based on the OMG Specification template [TEMPL]:

Section 0 of the submission shall be used to provide all non-normative supporting material relevant to the evaluation of the proposed specification, including:

- The full name of the submission
- A complete list of all OMG Member(s) making the submission, with a named contact individual for each
- The acronym proposed for the specification (e.g. UML, CORBA)
- The name and OMG document number of the RFP to which this is a response
- The OMG document number of the main submission document
- Overview or guide to the material in the submission
- Statement of proof of concept (see 4.8)
- If the proposal does not satisfy any of the general requirements stated in Section 5, a detailed rationale explaining why
- Discussion of each of the "Issues To Be Discussed" identified in Section 6.
- An explanation of how the proposal satisfies the specific requirements and (if applicable) requests stated in Section 6.

Section 1 and subsequent sections of the submission shall contain the normative specification that the Submitter(s) is/are proposing for adoption by OMG, including:

- Scope of the proposed specification
- Overall design rationale
- Conformance criteria for implementations of the proposed specification, clearly stating the features that all conformant implementations shall support, and any features that implementations may support, but which are not mandatory.
- A list of the normative references that are used by the proposed specification
- A list of terms that are used in the proposed specification, with their definitions
- A list of any special symbols that are used in the proposed specification, together with their significance

- The proposed specification itself

Section 0 will be deleted from any specification that OMG adopts and publishes. Therefore Section 0 of the submission shall contain no normative material, and any non-normative material outside section 0 shall be explicitly identified.

The main submission document and any models or other machine-interpretable files accompanying it shall be listed in an inventory file conforming to the inventory template [INVENT].

The submission shall include a copyright waiver in a form acceptable to OMG. One acceptable form is:

> "Each of the entities listed above: (i) grants to the Object Management Group, Inc. (OMG) a nonexclusive, royalty-free, paid up, worldwide license to copy and distribute this document and to modify this document and distribute copies of the modified version, and (ii) grants to each member of the OMG a nonexclusive, royalty-free, paid up, worldwide license to make up to fifty (50) copies of this document for internal review purposes only and not for distribution, and (iii) has agreed that no person shall be deemed to have infringed the copyright in the included material of any such copyright holder by reason of having used any OMG specification that may be based hereon or having conformed any computer software to such specification."

Other forms of copyright waiver may only be used if approved by OMG legal counsel beforehand.

4.10 How to Submit

Submitters should send an electronic version of their submission to the RFP Submissions Desk (rfp@omg.org) at OMG Headquarters by 5:00 PM U.S. Eastern Standard Time (22:00 GMT) on the day of the Initial and Revised Submission deadlines. Acceptable formats are Adobe FrameMaker source, ISO/IEC 26300:2006 (OpenDoc 1.1), OASIS DocBook 4.x (or later) and ISO/IEC 29500:2008 (OOXML, .docx).

Submitters should ensure that they receive confirmation of receipt of their submission.

5 General Requirements on Proposals

5.1 Requirements

5.1.1 Use of modeling languages

Submitters are encouraged to express models using OMG modeling languages such as UML, MOF, CWM and SPEM (subject to any further constraints on the types of the models and modeling technologies specified in Section 6 of this RFP). Submissions containing models expressed using OMG modeling

languages shall be accompanied by an OMG XMI [XMI] representation of the models (including a machine-readable copy). A best effort should be made to provide an OMG XMI representation even in those cases where models are expressed via non-OMG modeling languages.

5.1.2 PIMs & PSMs

Section 6 of this RFP specifies whether PIM(s), PSM(s), or both are being solicited. If proposals specify a PIM and corresponding PSM(s), then the rules specifying the mapping(s) between the PIM and PSM(s) shall either be identified by reference to a standard mapping or specified in the proposal. In order to allow possible inconsistencies in a proposal to be resolved later, proposals shall identify whether it's the mapping technique or the resulting PSM(s) that shall be considered normative.

5.1.3 Complete submissions

Proposals shall be precise and functionally complete. Any relevant assumptions and context necessary to implement the specification shall be provided.

5.1.4 Reuse

Proposals shall reuse existing OMG and other standard specifications in preference to defining new models to specify similar functionality.

5.1.5 Changes to existing specifications

Each proposal shall justify and fully specify any changes or extensions to existing OMG specifications necessitated by adopting that proposal. In general, OMG favors proposals that are upwards compatible with existing standards and that minimize changes and extensions to existing specifications.

5.1.6 Minimalism

Proposals shall factor out functionality that could be used in different contexts and specify their models, interfaces, etc. separately. Such minimalism fosters re-use and avoids functional duplication.

5.1.7 Independence

Proposals shall use or depend on other specifications only where it is actually necessary. While re-use of existing specifications to avoid duplication will be encouraged, proposals should avoid gratuitous use.

5.1.8 Compatibility

Proposals shall be compatible with and usable with existing specifications from OMG and other standards bodies, as appropriate. Separate specifications offering distinct functionality should be usable together where it makes sense to do so.

5.1.9 Implementation flexibility

Proposals shall preserve maximum implementation flexibility. Implementation descriptions should not be included and proposals shall not constrain implementations any more than is necessary to promote interoperability.

5.1.10 Encapsulation

Proposals shall allow independent implementations that are substitutable and interoperable. An implementation should be replaceable by an alternative implementation without requiring changes to any client.

5.1.11 Security

In order to demonstrate that the specification proposed in response to this RFP can be made secure in environments that require security, answers to the following questions shall be provided:

- What, if any, security-sensitive elements are introduced by the proposal?
- Which accesses to security-sensitive elements should be subject to security policy control?
- Does the proposed service or facility need to be security aware?

1. What default policies (e.g., for authentication, audit, authorization, message protection etc.) should be applied to the security sensitive elements introduced by the proposal? Of what security considerations should the implementers of your proposal be aware?

The OMG has adopted several specifications, which cover different aspects of security and provide useful resources in formulating responses. [SEC] [RAD].

5.1.12 Internationalization

Proposals shall specify the degree of internationalization support that they provide. The degrees of support are as follows:

a) Uncategorized: Internationalization has not been considered.

b) Specific to <region name>: The proposal supports the customs of the specified region only, and is not guaranteed to support the customs of any other region. Any fault or error caused by requesting the services outside of a context in which the customs of the specified region are being consistently followed is the responsibility of the requester.

c) Specific to <multiple region names>: The proposal supports the customs of the specified regions only, and is not guaranteed to support the customs of any other regions. Any fault or error caused by requesting the services outside of a context in which the customs of at least one of the specified regions are being consistently followed is the responsibility of the requester.

d) Explicitly not specific to <region(s) name>: The proposal does not support the customs of the specified region(s). Any fault or error caused by requesting

the services in a context in which the customs of the specified region(s) are being followed is the responsibility of the requester.

5.2 Evaluation criteria

Although the OMG adopts model-based specifications and not implementations of those specifications, the technical viability of implementations will be taken into account during the evaluation process. The following criteria will be used:

5.2.1 Performance

Potential implementation trade-offs for performance will be considered.

5.2.2 Portability

The ease of implementation on a variety of systems and software platforms will be considered.

5.2.3 Securability

The answer to questions in section 5.1.11 shall be taken into consideration to ascertain that an implementation of the proposal is securable in an environment requiring security.

5.2.4 Conformance: Inspectability and Testability

The adequacy of proposed specifications for the purposes of conformance inspection and testing will be considered. Specifications should provide sufficient constraints on interfaces and implementation characteristics to ensure that conformance can be unambiguously assessed through both manual inspection and automated testing.

5.2.5 Standardized Metadata

Where proposals incorporate metadata specifications, OMG standard XMI metadata [XMI] representations should be provided.

6 Specific Requirements on Proposals

6.1 Problem Statement

6.1.1 General Overview

This RFP addresses the emerging semantic interoperability problems encountered around operational Threats and Risks, including their Management and Assessment.

A key component of operational risk is risk from threat actors. Threat actors have become increasingly more advanced and sophisticated in their techniques and strategies. The campaigns of these threat actors are long term, multi-phased and combine physical and cyber tactics directed at multiple targets. Intentional threats from threat actors can be combined with natural threats. Threat activities are described by multiple patterns, applied to multiple forms of observation (including automated sensors and human observations). The management and mitigation of threats and risks is a cross-cutting concern spanning commercial, federal, state, local and tribal entities.

Systematic offline assessment of risks for a given system and organization, selecting and implementing a proactive mitigation strategy, and performing dynamic monitoring, assessing and reaction to imminent and ongoing attacks involves analysis and management of large collections of data. Some data is held internally where as other data is shared based on policy, agreements and shared interest.

Monitoring for threat activities involves monitoring large sets of indicators and analysis of data over a significant period of time.

Within the intelligence community the "intelligence cycle" has been recognized as central to effective risk management. The intelligence cycle is depicted on the right; showing the cycle of collaboration from requirements gathering through dissemination. The 'intelligence cycle' forms the core of the baseline capabilities for the National Network of Fusion Centers and is used for threat analysis and risk mitigation[4].

1 Intelligence Cycle

Various communities have started addressing these issues by developing ecosystems[5] for threat information sharing. While non-cyber domains (specifically the intelligence and related communities) have a rich history of threat analysis and

[4] http://www.it.ojp.gov/documents/baselinecapabilitiesa.pdf

information sharing, the massive proliferation of automated machine-speed attack capabilities is putting heavy strains on traditional threat and risk evaluation and mitigations techniques. At the same time, different communities (such as IT/cyber, law enforcement, emergency management, business architecture, etc.) are developing different approaches to address this challenge. As a result, different taxonomies, models, and protocols have emerged that address the specific needs of the respective community yet create stovepipes for the overall ecosystem.

Threat actors do not respect community boundaries, they exploit them. What is needed is a broad-based solution that federates a wide range of threat and risk concerns to arrive at the appropriate courses of action and mitigation strategies. The Intelligence Reform and Terrorism Prevention Act of 2004[6] along with the findings and recommendations of the Markel Foundation[7] highlight these principles.

In planning for and analyzing threats and risks, we need to understand and share information for planning, contingencies and forensics. Simulations then add to our capability to evaluate other threats, risks and courses of action. All of these concerns should then be federated in a broad-based threat and risk model.

6.1.2 Operational Risk Management

In the broadest sense, organizations manage risks in order to provide a systematic response to uncertainties. Operational risk focuses on risks due to possible threats or undesired natural occurrences. Many organizations conduct their business within regulatory frameworks that obligate them to safeguard certain assets in accordance with standards and perform threat and risk assessment. Risk Management is conducted to identify, assess and mitigate hazards resulting from any uncertain event that may occur and result in adverse consequences that may affect stakeholders. In the context of a system life cycle, Risk Management can focus on the adverse events at various stages of the system life cycle, and therefore address different kinds of risk, such as the Project Management Risk (where the adverse events affect system cost, schedule and technical characteristics before the system utilization stage can start) and Operational Risk (where the adverse events affect the success of a mission or organization in real time). The design goal of this RFP is limited to the risk related to the operational portion of the life-cycle.

Typical Risk Management Outcomes include:

1) Risk management plan.

2) Risks identified, categorized, prioritized and status allocated.

---

[5] An ecosystem in this context is a community of stakeholders combined with their supporting technologies and practices

[6] http://ise.gov/sites/default/files/IRTPA_amended.pdf

[7] Markle Foundation: http://www.markle.org/news-events/connected-world-blog/creating-information-sharing-environment-status-implementation

3) Appropriate risk management strategies defined.

4) Action taken to mitigate or avoid the impact of risk.

Several conceptual frameworks have been developed that describe the elements of threat and risk analysis (including risk identification, assessment and evaluation). These frameworks allow organizations to define the risks in terms of their dimensions, e.g. technical, programmatic, organizational, financial, information quality and within these dimensions, to select the method for expressing risks in suitable terms.

Methodologies for risk management describe activities that identify risks to predict what could go wrong and would adversely affect the system and the organization. This usually involves identifying the initiating events associated with each risk in each risk category. Risk identification then proceeds by defining the interrelationships between sources of risk where there is any coupling. This may be based on project/product histories, checklists, questionnaires and expert analysis. Risk assessment methodologies describe how to conduct a frequency analysis of initiating event occurrence to identify the likelihood of risk occurrence. A risk assessment methodology will also describe steps to evaluate the impact of the risks and define their possible adverse consequences. Risk management involves prioritization of the risks in terms of their likelihood and possible impact. An organization would usually define a threshold of tolerability for each risk category.

Successful risk assessment is based upon detailed understanding of the operational environment of the system and the organization.

Multiple communities have developed protocols, including data and exchange schema and interfaces for sharing information about threats, risks and incidents that impact important government, commercial and personal assets and privacy. While each of these schema and interfaces provides value for a specific community it is difficult to federate these multiple representations to arrive at broad-based, planning, simulation, assessment, situational awareness, and forensics and to then enact the appropriate courses of action. Cyber related attacks have added a new dimension that stresses traditional mitigation strategies.

However, several comparative studies of the existing risk analysis methodologies and frameworks have concluded that the existing methodologies, even if based on similar principles, differ in their knowledge bases (assets, threats, vulnerabilities, ...) or type of results (quantitative or qualitative). This makes the risk assessments difficult or impossible to compare when different methods have been used. This makes it difficult to exchange threat and risk related information between multiple communities.

6.1.3 This RFP

This RFP requests submissions that include a conceptual model for operational threats and risks that is intended to provide a “pivot point” across multiple existing and evolving

threat and risk sharing schema and interfaces. This conceptual model will be informed by the existing standards and best practices such that the information that needs to be shared across communities can be federated together and presented to planners, analysts and others – thereby protecting assets in a coherent framework. Existing work that will inform this conceptual model include but are not limited to STIX and NIEM, Common Weakness Enumerations and ISO 31000. References to these other specifications can be found in section 6.2.4.

This conceptual model will then be mapped to a NIEM data model which will provide a concrete exchange format using the NIEM reference models and technical architecture. The NIEM representation will provide full coverage of the concepts in the conceptual model and can be used for cross-domain interoperability. However, due to the conceptual model approach, information sharing is not limited to NIEM-only.

By defining a comprehensive conceptual model, such a model will allow the creation of a generic mapping from the domain specific models to and from the conceptual model. This in turns enables the ability to create semantically consistent mappings across communities, data models and domains.

6.1.4 Specific Use Cases

In support of the overall scope, the following use cases will guide the development of the specification. While a solution is not required to satisfy all, or even any specific use case, it will be evaluated on how many different use cases it actually can address. Use cases and detail are being developed by the community on:

- https://github.com/omg-threat-modeling/phase1

While this RFP requests responses for a thin and wide model that captures the concepts of threat modeling and risk management, these use cases provide real life applications, solutions, and capabilities that would allow for specific elements from the underlying technical specifications to be integrated and modelled as needed.

6.2 Scope of Proposals Sought

The purpose of this initiative is to develop a computation independent model (CIM) as a conceptual model to represent a broad, semantically aligned view of threat and risk across multiple domains and segments. Most communities have their own preferred formats and mechanisms for representing and sharing information about threat. The conceptual model will be mapped to platform specific representations (e.g. XML Schema) through their logical model representation (PIM) to drive semantic interoperability across multiple formats supporting cross-domain mission and use-case requirements. This cross-domain capability will then provide a framework that will aid in planning, simulation, assessment, situational awareness and integrated threat/risk response.

6.2.1 Operational vs. other kinds of threats and risks

This RFP requests models for operational threats and risks. Operational risks are situations having a negative impact on an organization or company due to uncertainties related to possible breakdowns in a system or its environment via supply chain, injury to a person or failure of a process resulting from intentional/malicious as well as

unintentional/natural operational threats. One of the main impacts of operational risks is inability to conduct operations as planned.

Examples of operational risks and threats include but are not limited to: Danger to an oil rig from a hurricane, an organizations loss of private or confidential information, an attack on a power substation potentially causing grid failure, compromise of industrial control systems, threat of physical and/or cyber-attacks on major sporting events, denial of service attacks on a web site, etc.

Operational threats and risks may be distinguished from other kinds of business risks such as market risk, credit risk, legal risk, project management risk or reputation risk.

6.2.2 Types of threats and risks which are in scope

Specifically, the following should be addressed at the conceptual level:

- Ensure that the conceptual threat/risk model can be applied to different domains, specifically:
    - Cyber/information and communication systems and assets
    - Physical systems and assets, including embedded and manufacturing
    - Electromagnetic spectrum assets (E.g. interference with wireless systems or radio)
- Ensure that the model can be applied to the following communities and systems:
    - Public & Private sector, including
        - Information systems
        - Facilities management
        - Financial systems
        - Logistic underpinnings for supply chains
    - Law enforcement at the national, state, local, tribal, territorial, and international level
    - General emergency management
    - Industrial control systems
- Ensure that the Threat and Risk Model can be applied to actor-less threats, specifically those representing natural threats
- Considerations across the threat/risk life-cycle
    - Identifying and planning for risks at the enterprise level
    - Vulnerabilities due to software, process or policy failure
    - Insider threats
    - Terrorist threats
    - Continuous diagnostics & Monitoring
    - Contingency planning

- Simulation
- Forensics

Additionally, the following applications SHOULD be addressed:

- Capabilities to account for the following threat domains or communities
  - Chemical threats
  - Biological and medical threats
  - Radiological threats
  - Nuclear threats
- Ensure that the following additional communities can leverage the model:
  - Military communities and systems
  - Intelligence communities and systems
  - Pandemic emergency management

6.2.3 Level of detail

Any of the above threats and risks can be represented at various levels of detail and granularity. The purpose of this RFP is not to capture every possible concept and property of all of the above domains, as that would be both overwhelming and redundant. The models defined in RFP responses should cover the high-level concerns of these domains such that summary level and cross-domain information sharing is actionable and enabled. The concepts defined should provide a foundation for further elaboration by specific communities. Where detail is not included, mechanisms should be provided to reference more detail in domain specific specifications.

For example, since the cyber threat domain is new and critical, more detail is expected for cyber concepts that will be expected to be shared by the cyber community. However extremely fine-grain and technology specific information is captured in current specifications and is not expected to be replicated.

The level of detail and degree of abstraction across domains is a judgment call on the part of submitters. Submitters will be asked to discuss their design choices with respect to degree of detail and abstraction.

6.2.4 Informative specifications and schema

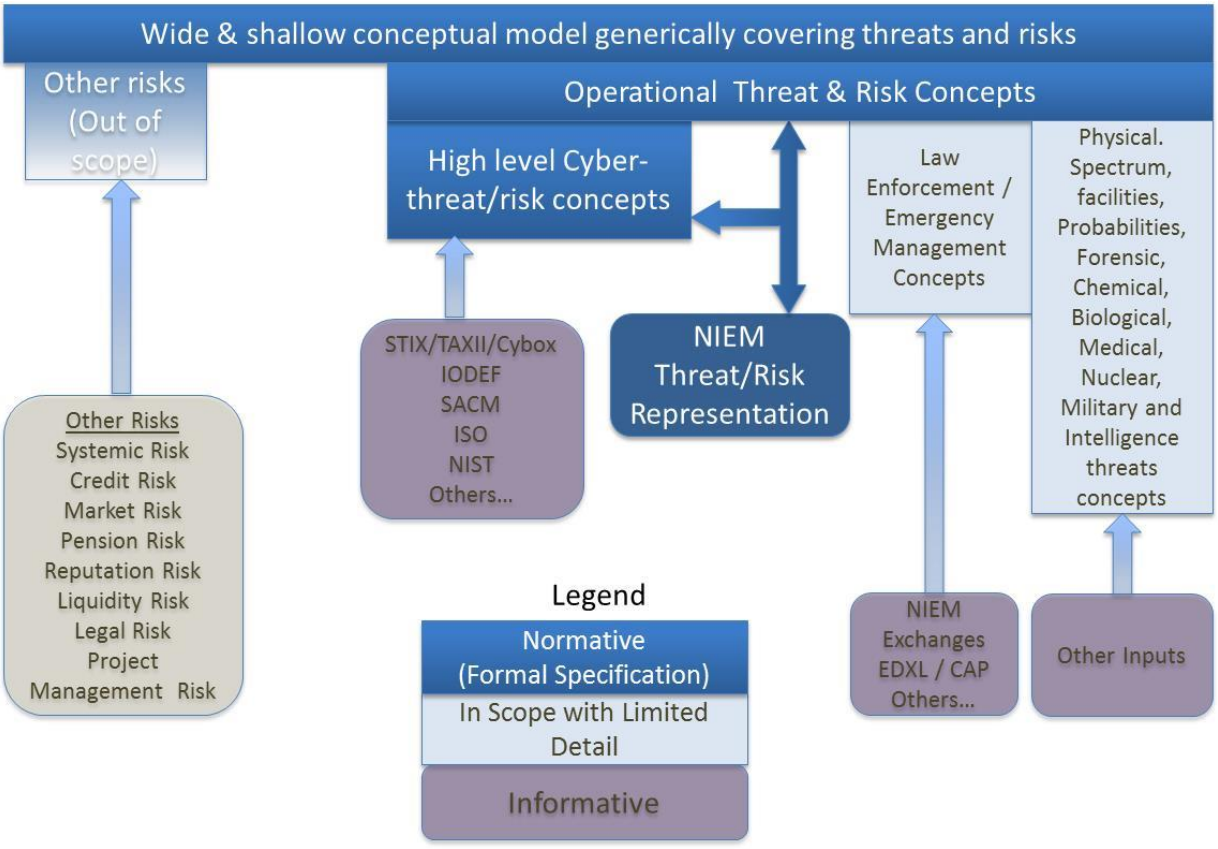
As there has been substantial work in specific domains with regard to threats and risks, the proposed models should be informed by existing specifications for defining the conceptual model and NIEM mapping. These informative specifications include but are not limited to those found in section 6.4.

6.2.5 Conceptual model and mappings

The approach being requested in this RFP is based on utilizing a “conceptual model”, expressed in UML, to capture the concepts relevant to threats and risks across multiple

domains and communities. The conceptual model will be layered and modular to allow for specific areas of concerns and domains to successively add detail to general concepts and relationships as required. The design focus of the conceptual model will be "operational threats and risks" with specific attention to high-level cyber related threats and risks. The conceptual model should then be able to be used to "semantically ground" specific exchange specifications such that the concepts shared between different exchange representations used by different communities may be understood and mapped. As each of these exchange standards is designed with specific structures, design choices and technologies in mind – the conceptual model should be free of such commitments. The conceptual model will then be "mapped" to each representation (PIM or PSM) to be federated. PIM or PSM models may be expressed in UML, XML or ontological languages.

Specifications may utilize, extend or define UML profiles to express the conceptual and mapping semantics. Submissions may use the SIMF (Semantic Information Modeling for Federation) specification if it is sufficiently defined at submission time. Such profiles will then be used to define and map the threat/risk models.



2 Operational Threat and Risk Scope

The above graphic illustrates the expected scope of this RFP. Note that later RFPs may extend the scope to "drill down" into other kinds of threats and risks.

6.2.5.1 Wide and shallow conceptual model generically covering threats and risks

The "wide and shallow" conceptual model(s) will cover threats and risks in general, as well as supporting concepts. These models should be informed by all of the domains listed in section 6.2.2~~6.2.1~~ and be able to represent summary and cross-domain information of interest. This model is to contain minimal detail to provide the broadest possible interpretations of threats and risks. It is the expectation that this model will be extended to more specific areas of interest or domains such as operational risk and/or business marketplace risk.

6.2.5.2 Operational threat and risk concepts

The operational threat and risk conceptual model will extend the more generic concepts to focus on operational threat and risk concepts as the focus of this RFP. While this model is more specialized it is still considered cross-domain and is not expected to be deep. This layer will be the basis for cross-domain information sharing of operational threats and risks.

6.2.5.3 High-level Cyber threat/risk concepts

Additional conceptual level granularity and detail is to be provided by the Cyber domain. The primary input to this level is expected to be the high-level concepts of the Cyber domain (e.g. as defined in STIX), however submitters are free to utilize other specifications. Formal mappings to STIX and non-normative mappings to SAR[8] are to be provided as proofs of concept.

6.2.5.4 NIEM[9] Threat/Risk Representation

NIEM EIEM[10]s, reference models and/or IEPD[11]s are to be defined in submissions to this RFP that provide for a NIEM specific representation of the complete conceptual model such that NIEM implementations will be able to share threat/risk information from multiple sources and across communities. The NIEM representation shall utilize existing NIEM reference models as applicable.

The conceptual model provides a pivot point between the multiple possible representations of operational threat and risk information but does not define a specific information exchange format. To provide at least one concrete representation in XML schema, the conceptual model will be mapped to NIEM using NIEM-UML. NIEM-UML defines how these UML models will then map to NIEM conformant XML schema. This

---

[8] SAR: Suspicious Activity Report, a NIEM IEPD.

[9] NIEM: National Information Exchange Model – http://www.niem.gov

[10] A NIEM EIEM is a reusable business data model in NIEM format

[11] A NIEM IEPD is an Information Exchange Package Description which documents an information sharing data structure

will then provide for a full NIEM-XML representation of the covered threat and risk concepts.

As NIEM is well established as the U.S. information exchange model in justice and public safety, the NIEM representation will enable interactions with that community in a language and format they understand.

NIEM will also be used as a reference for domain concepts to populate the conceptual model. NIEM provides well developed and stakeholder vetted definitions for cross-domain concepts.

6.2.6 Follow on efforts

This RFP is part of a multi-phased initiative that will later leverage the risk/threat conceptual model to drill down into more specific threat and risk domains (areas of interest) with more detail.

Follow-on efforts are expected to extend the level of granularity and mapping of other exchange formats.

More information about the Threat Model work in progress can be found at:

- https://github.com/omg-threat-modeling/phase1

6.3 Relationship to other OMG Specifications and activities

6.3.1 Relationship to OMG specifications

The following specifications should be considered for their relationship to the UML Profile for Threat Information Sharing:

6.3.1.1 Unified Modeling Language (UML) - http://www.omg.org/spec/UML/. UML provides the extensible and accepted modeling framework for use in threat and risk modeling.

6.3.1.2 Object Constraint Language (OCL) – http://www.omg.org/spec/OCL/. OCL provides a language for specifying constraints in models.

6.3.1.3 Unified Profile for DoDAF/MODAF (UPDM) - http://www.omg.org/spec/UPDM/. UPDM is the UML representation of the Defense architectural standards DoDAF and MODAF which may contain related concepts.

6.3.1.4 Meta Object Facility (MOF 2.4) - http://www.omg.org/spec/MOF/. MOF provides a framework for meta-modeling in which the abstract syntax of UML and other modeling languages is described.

6.3.1.5 XML Metadata Interchange (XMI®) - http://www.omg.org/spec/XMI/. XMI provides a XML interchange format for MOF models.

6.3.1.6 Query/View/Transformation (QVT) - http://www.omg.org/spec/QVT/. QVT is the OMG standard for expressing model transformation rules.

6.3.1.7 MOF Models to Text Transformation Language - http://www.omg.org/spec/MOFM2T/. Model to text provides a way to specify transformation of models to textual representations.

6.3.1.8 CWM – Common Warehouse Metamodel- http://www.omg.org/spec/CWM/. CWM defines a metamodel for common data modeling schema

6.3.1.9 SBVR - Semantics of Business Vocabulary and Business Rules (SBVR) - http://www.omg.org/spec/SBVR/. SBVR specifies a model for defining business vocabulary and rules

6.3.1.10 Shared Operational Picture Exchange Services, (SOPES) Information Exchange Data Model (IEDM) - http://www.omg.org/spec/SOPES/.

6.3.1.11 Model Driven Message Interoperability (MDMI) - http://www.omg.org/spec/MDMI/. MDMI provides a standard for financial message definition and mapping.

6.3.1.12 Ontology Definition Meta Model (ODM) – http://www.omg.org/spec/ODM/. ODM provides MOF and UML representations of multiple ontology languages including OWL, RDF/S and Common Logic.

6.3.1.13 Structured Assurance Case Metamodel (SACM) - http://www.omg.org/spec/SACM/. Assurance cases include many concepts overlapping with threats and risks that submitters may consider.

6.3.1.14 Financial Industry Business Ontology (FIBO) – FIBO provides a conceptual ontology that includes concepts of financial risk. http://www.omg.org/spec/EDMC-FIBO/. While financial risk is out of scope submitters are encouraged to consider possible use of related vocabulary and definitions.

6.3.1.15 Business Motivation Metamodel (BMM) – http://www.omg.org/spec/BMM/. BMM provides concepts for means and ends that may be appropriate for risks.

6.3.1.16 UML Profile for NIEM (NIEM-UML) - http://www.omg.org/spec/NIEM-UML/. NIEM UML provides the foundational models for NIEM exchanges relating to threats and risks.

6.3.2 Relationship to other OMG Documents and work in progress

6.3.2.1 *Information Management Metamodel (IMM) (http://www.omg.org/techprocess/meetings/schedule/IMM_RFP.html).* IMM

will include a metamodel for XML schema that can be used with a QVT *mapping*

6.3.2.2 UML Profile for NIEM (NIEM-UML) 3.0. (http://www.omg.org/techprocess/meetings/schedule/UML_Profile_for_NIEM_3_RFP.html) Note, this is a follow-on effort for the existing NIEM profile based on NIEM- 2.1.

6.3.2.3 Semantic Information Modeling for Federation (SIMF) –SIMF will provide a foundation for conceptual modeling and mapping:

6.3.2.4 http://www.omgwiki.org/architecture-ecosystem/doku.php?id=semantic_information_modeling_for_federation_rfp

6.3.2.5 Information Exchange Framework (IEF) Reference Architecture: http://www.omg.org/cgi-bin/doc.cgi?mars/2014-3-17. – IEF will specify a Reference Architecture to guide the development of related specifications in the domain of policy driven, data-centric information sharing and safeguarding (ISS) services.

6.4 Related non-OMG Activities, Documents and Standards

6.4.1.1 STIX– The STIX (Structured Threat Information Expression) set of specifications has been developed in a community effort to represent information sharing structures for Cyber-attacks: http://stix.mitre.org

6.4.1.2 IETF IODef - Incident Object Description Exchange Format: http://www.ietf.org/rfc/rfc5070.txt

6.4.1.3 OpenIOC – Open Framework for Sharing Threat Intelligence: http://www.openioc.org/

6.4.1.4 OASIS Common Alerting Program & EDXL: https://www.oasis-open.org/committees/download.php/17227/EDXL-DE_Spec_v1.0.html

6.4.1.5 EMAP Emergency Management Standard: http://www.emaponline.org/index.php?option=com_content&view=article&id=118&Itemid=110

6.4.1.6 Security Fabric Alliance: http://sfsig.omg.org/index.htm

6.4.1.7 NIEM Related Domain IEPDs: http://www.NIEM.GOV

6.4.1.8 SO 31000 – Risk Management: http://www.iso.org/iso/home/standards/iso31000.htm

6.4.1.9 FISMA - Federal Information Security Management Act (FISMA) Implementation Project: http://csrc.nist.gov/groups/SMA/fisma/framework.html

6.4.1.10 NIEM Reference models and IEPDs – NIEM provides for information sharing across multiple domains and has specific concepts relating to law enforcement, emergency management and terrorism prevention: http://www.niem.gov

6.4.1.11 SAR – Suspicious Activity Report: http://nsi.ncirc.gov

6.4.1.12 Emergency Data Exchange Language (EDXL) Standards from Oasis: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency

6.4.1.13 ISO/IEC 13335: Information technology -- Security techniques -- Management of information and communications technology security

6.4.1.14 ISO/IEC 15408: Information technology -- Security techniques -- Evaluation criteria for IT security

6.4.1.15 ISO/IEC 15443: Information technology -- Security techniques -- Security assurance framework

6.4.1.16 ISO/IEC 27001: Information technology -- Security techniques -- Information security management systems -- Requirements

6.4.1.17 Common Weakness Enumerations (CWE): http://cwe.mitre.org/

6.4.1.18 EBIOS: (French: Expression des besoins et identification des objectifs de sécurité) allows evaluation and action on risks relative to information systems security, and proposes a security policy adapted to the needs of an organization.

6.4.1.19 HTRA (Canada): High Throughput Risk Assessment

6.4.1.20 NIST SP-800-30 (US): Guide for Conducting Risk Assessments

6.4.1.21 Octave (SEI CMU): Operationally Critical Threat, Asset, and Vulnerability Evaluation

6.4.1.22 Microsoft Threat Analysis Tool

6.5 Mandatory Requirements

6.5.1 Conceptual models

6.5.1.1 Submissions shall define modular UML conceptual models to specify the concepts required to represent information about operational threats and risks.

6.5.1.2 The conceptual model shall capture the intended meaning of operational threat and risk related concepts such that it may be used as a reference for the use of those concepts in specific exchanges and data stores.

6.5.1.3 The conceptual model shall not assume any particular technology, domain, representation, structure of information or schema. It shall be a model of the concepts representing real-world entities, not of a specific data representation.

6.5.2 Operational Threat and Risk concepts

6.5.2.1 The conceptual models shall provide definitions of the concepts of "operational threats" and "operational risk". Proposals shall use standard terminology when applicable. References to existing standards shall be provided to facilitate mappings and avoid ambiguity.

6.5.2.2 Proposal's conceptual models shall define other concepts related to common operational threat and risk terms including but not limited to:

- Asset
- Campaign
- Cause
- Effect
- Exploit target
- Goal

- Hazard
- Impact
- Incident
- Indicator
- Likelihood
- Mitigation
- Observable
- Observation
- Observation metadata
- Procedures
- Risk
- Safeguard
- Severity
- Strategy
- Tactics
- Techniques
- Threat
- Threat actor
- Threat source
- Undesired event

Note that proposals are required to cover the above enumerated list in the conceptual models but are not required to use the same terms. Where differing terms are used, submissions shall explain how their terms and concepts relate to the above.

6.5.2.3 The concepts of threats shall include the following classifications:

- Cyber/information and communication systems and assets
- Physical systems and assets, including embedded and manufacturing
- Electromagnetic spectrum assets (E.g. interference with wireless systems or radio)
- Industrial control systems

6.5.2.4 Models for operational threats and risks shall be consistent with the following constraints:

- Defensive, offensive, or other actors may or may not have insight into the plans or strategies of the respective other actors. As such, model implementations will in those cases be incomplete and rely on estimates and assumed parameters.
- Models must be able to support non-actor threats (such as natural disasters) that will not be associated with any coherent intentions or plans.
- Bystanders and inadvertent actors may perform actions that result in behavior that provides benefits to any other actor (offensive or defensive). Such actions are understood to be non-intentional.
- The focus of risks will be those that go beyond the normal course of business and expose the enterprise to increased risk due to threats & vulnerabilities.

6.5.2.5 Models for operational threats and risks shall include concepts for expressing probability and/or confidence levels (e.g. for likelihood of occurrence and impact)

6.5.3 Risk Management concepts

6.5.3.1 The conceptual model shall include concepts related to systematic identification of operational risks and assessing their likelihood and severity.

6.5.3.2 The proposals shall include concepts related to prioritization of risks.

6.5.3.3 The proposals shall include concepts related to the mapping of risks, hazards and undesired events to descriptions of systems for the purpose of systematic hazard analysis and justifiable identification of risks.

6.5.3.4 The proposals shall describe concepts related to exchange of risk indicators, including patterns for systematic identification of risks.

6.5.4 Mitigation and courses of action

6.5.4.1 The conceptual models shall include concepts of "course of action" and mitigation of threats and risks.

Explanation: Coincident with understanding any threat or risk is taking steps to mitigate the specific threat and mitigate similar risks in the future. The conceptual models for "course of action" and mitigation shall include corrective concepts for deterring, protecting, detecting, monitoring, limiting, preventive and recovery strategies and courses of action.

6.5.5 Threat and Risk planning

6.5.5.1 The conceptual model shall include concepts for understanding, planning for and treating operational risks, threats and their contingencies at the governmental and enterprise level.

6.5.6 NIEM Representation and mapping

6.5.6.1 Submissions shall define a normative NIEM-UML PIM representation sufficient to capture the concepts as defined in the conceptual models as defined above.

6.5.6.2 This NIEM-UML representation shall be mapped to the conceptual models such that the meaning of each threat/risk relevant NIEM element is described in the conceptual model.

6.5.6.3 The mapping shall be sufficiently expressive such that any set of instances represented in or logically mapped to the conceptual model shall be able to be represented in NIEM (understanding that choices and rules will have to be made).

6.5.6.4 Any instance of the NIEM specification shall be able to be logically mapped to the conceptual model.

6.5.7 STIX mapping

6.5.7.1 Submissions shall define a mapping to the subset of STIX that corresponds with the conceptual model. This mapping shall demonstrate that the conceptual model is sufficient to represent high-level STIX concepts.

6.5.8 Common requirements

6.5.8.1 All models shall utilize UML and UML profiles as a foundation.

6.5.8.2 Concepts that are required for understanding threats or risks should, as much as possible, be defined in a modular fashion such that these concepts may be reused for related threat/risk concepts NIEM and other reference models shall be used as a reference for such cross-domain concepts. It is understood that a model may be composed of multiple sub-models.

6.6 Non-mandatory requirements

6.6.1 Optional mappings

Submissions may provide normative or non-normative mappings to support the following Platform Specific Models, or logical models for the following protocols or communities:

- OASIS Common Alerting Program & EDXL
- Others as deemed important by submitters

6.6.2 Optional support for conceptual modeling and mapping

Submissions may reference and/or define non-normative UML profiles and associated QVT (or other ways to express mapping logic) for conceptual modeling and the mapping.

Submitters are encouraged to follow the progress of and use as appropriate SIMF, ODM, MDMI, semantic web and other efforts to help define conceptual model and mappings.

6.6.3 Optional MOF representation

Submissions may define A MOF metamodel that utilizes the conceptual model and provides an XMI representation of Operational Threats and Risks.

6.6.4 Optional Integration with UPDM

Submissions may define conceptual integration points with UPDM.

6.7 Issues to be discussed

6.7.1 Simulation

Submissions shall discuss how the models could be used for simulation. The intent is to support the use of complex simulation systems (e.g. Monte Carlo methods) to test multiple scenarios.

6.7.2 Applicability

Submissions shall discuss the applicability of their approach to possible future efforts to embrace other domains, specifications or levels of detail related to threats and risks.

6.7.3 Design choices

Submissions shall discuss their design choices for level of detail.

6.8 Evaluation Criteria

6.8.1 Situational Awareness

Submissions shall be evaluated based on their ability to support broad-based situational awareness about operational threats and risks and represent appropriate courses of action.

6.8.2 Enterprise planning, assessment and architecture

Submissions shall be evaluated based on their applicability to support the planning and assessment for operational risks, threats and mitigations.

6.8.3 Completeness

Submissions shall be evaluated based on the completeness of the representation of operational threat and risk concepts

6.8.4 Fidelity

Submissions shall be evaluated based on their proof of fidelity with existing operational threat and risk specifications and best practices.

6.8.5 Extensibility

Submissions shall be evaluated based on the ability of their approach to be extended to other domains and more detailed levels of granularity in future efforts.

6.8.6 Fit for purpose as defined by use cases

Submissions shall be evaluated based on their ability to support the use cases referenced in section 6.1.4.

6.8.7 Understandability

Submissions shall be evaluated based on the ability of non-technical stakeholders to understand the conceptual model and for technologists to understand the relationship of those models to their technology frameworks and representations.

6.9 Other information unique to this RFP

None

6.10 IPR Mode

The IPR Mode for this initiative will be Non-Assert Covenant

Every OMG Member that makes any written Submission in response to this RFP shall provide the Non-Assertion Covenant found in Appendix A of the OMG IPR Policy [IPR].

6.11 RFP Timetable

The timetable for this RFP is given below. Note that the TF or its parent TC may, in certain circumstances, extend deadlines while the RFP is running, or may elect to have more than one Revised Submission step. The latest timetable can always be found at the OMG Work In Progress page at http://www.omg.org/schedules under the item identified by the name of this RFP.

Event or Activity	Planned Date
Release of RFP Draft for Review and Comment	*May 2nd, 2014*
Complete DRAFT RFP	*May 12th, 2014*
RFP final review and comment	*May 15th, 2014*
RFP placed on OMG document server	*May 16th, 2014*
Approval of RFP by Architecture Board *Review by TC*	*June 16th, 2014*
TC votes to issue RFP	*June 17th, 2014*
LOI to submit to RFP due	*January 5th 2015*
Initial Submissions due and placed on OMG document server ("Four week rule")	*February 23rd , 2015*
Initial Submission presentations	*March 23rd, 2015*
Voter registration closes	*April 15th , 2015*
Preliminary evaluation	*June 15th, 2015*
Revised Submissions due and placed on OMG document server ("Four week rule")	*August 24th, 2015*
Revised Submission presentations	*September 21st, 2015*
Final evaluation and selection by TF *Recommendation to AB and TC*	*September 22nd, 2015 {If vote to vote can be obtained, otherwise December 7th 2015}*
Approval by Architecture Board *Review by TC*	*September 24th, 2015*
TC votes to recommend specification	*December, 2015*
BoD votes to adopt specification	*March, 2016*

Appendix a References & Glossary Specific to this RFP

A.1 References Specific to this RFP

None other than those specified above.

A.2 Glossary Specific to this RFP

The following definitions are informative and may be redefined by submissions.

- **Conceptual Model**: A model of the concepts relative to a domain of interest. A conceptual model models the "real world", not data or technology.
- **Operational Risk**: Operational risks are situations having a negative impact on an organization or company due to uncertainties related to possible breakdowns in a system or its environment via supply chain, injury to a person or failure of a process resulting from intentional/malicious as well as unintentional/natural operational threats. One of the main impacts of operational risks is inability to conduct operations as planned.
- **Operational Threat**: Operational threats involve specific incidents or groups of incidents that cause unwanted loss or harm to people or important assets or groups of assets. These incidents may be caused by threat actors, accidents or natural phenomenon. Examples include terrorist attacks, hurricanes or an electrical grid failure.
- **Risk**: Risks are situations with inherent uncertainty having a negative impact on objectives, people or assets.
- **System**: A system is a collection of parts and relationships among these parts that may be organized to accomplish some purpose. Systems include organizations, governments, people, processes, communities and information systems.
- **Threat**: any potential event or act, deliberate, accidental or natural hazard that could cause injury to people or assets, and thereby affect operations adversely.
- **Domain**: A specific sphere of concern, activity or knowledge.
- **Cyber**: of, relating to, or characteristic of the culture of computers, information technology, and virtual reality.

Appendix B General Reference and Glossary

B.1 General References

The following documents are referenced in this document:

[BCQ] OMG Board of Directors Business Committee Questionnaire, http://doc.omg.org/bcq

[CCM] CORBA Core Components Specification
http://www.omg.org/spec/CCM/

[CORBA] Common Object Request Broker Architecture (CORBA)
http://www.omg.org/spec/CORBA/

[CORP] UML Profile for CORBA,
http://www.omg.org/spec/CORP

[CWM] Common Warehouse Metamodel Specification
http://www.omg.org/spec/CWM

[EDOC] UML Profile for EDOC Specification
http://www.omg.org/spec/EDOC/

[Guide] The OMG Hitchhiker's Guide
http://doc.omg.org/hh

[IDL] Interface Definition Language Specification
http://www.omg.org/spec/IDL35

[INVENT] Inventory of Files for a Submission/Revision/Finalization
http://doc.omg.org/inventory

[IPR] IPR Policy
http://doc.omg.org/ipr

[ISO2] ISO/IEC Directives, Part 2 – Rules for the structure and drafting of International Standards
http://isotc.iso.org/livelink/livelink?func=ll&objId=4230456

[LOI] OMG RFP Letter of Intent template
http://doc.omg.org/loi

[MDAa] OMG Architecture Board, "Model Driven Architecture - A Technical Perspective"
http://www.omg.org/mda/papers.htm

[MDAb] Developing in OMG's Model Driven Architecture (MDA)
http://www.omg.org/mda/papers.htm

[MDAc] MDA Guide
http://www.omg.org/docs/omg/03-06-01.pdf

[MDAd] MDA "The Architecture of Choice for a Changing World
http://www.omg.org/mda

[MOF] Meta Object Facility Specification
http://www.omg.org/spec/MOF/

[NS] Naming Service
http://www.omg.org/spec/NAM

[OMA] Object Management Architecture
http://www.omg.org/oma/

[OTS] Transaction Service
http://www.omg.org/spec/OTS

[P&P] Policies and Procedures of the OMG Technical Process
http://doc.omg.org/pp

[RAD] Resource Access Decision Facility
http://www.omg.org/spec/RAD

[ISO2] ISO/IEC Directives, Part 2 – Rules for the structure and drafting of International Standards
http://isotc.iso.org/livelink/livelink?func=ll&objId=4230456

[RM-ODP]
ISO/IEC 10746

[SEC] CORBA Security Service
http://www.omg.org/spec/SEC

[TEMPL] Specification Template
http://doc.omg.org/submission-template

[TOS] Trading Object Service
hptp://www.omg.org/spec/TRADE

[UML] Unified Modeling Language Specification,
http://www.omg.org/spec/UML

[XMI] XML Metadata Interchange Specification,
http://www.omg.org/spec/XMI

B.2 General Glossary

Architecture Board (AB) - The OMG plenary that is responsible for ensuring the technical merit and MDA-compliance of RFPs and their submissions.

Board of Directors (BoD) - The OMG body that is responsible for adopting technology.

Common Object Request Broker Architecture (CORBA) - An OMG distributed computing platform specification that is independent of implementation languages.

Common Warehouse Metamodel (CWM) - An OMG specification for data repository integration.

CORBA Component Model (CCM) - An OMG specification for an implementation language independent distributed component model.

Interface Definition Language (IDL) - An OMG and ISO standard language for specifying interfaces and associated data structures.

Letter of Intent (LOI) - A letter submitted to the OMG BoD's Business Committee signed by an officer of an organization signifying its intent to respond to the RFP and confirming the organization's willingness to comply with OMG's terms and conditions, and commercial availability requirements.

Mapping - Specification of a mechanism for transforming the elements of a model conforming to a particular metamodel into elements of another model that conforms to another (possibly the same) metamodel.

Metadata - Data that represents models. For example, a UML model; a CORBA object model expressed in IDL; and a relational database schema expressed using CWM.

Metamodel - A model of models.

Meta Object Facility (MOF) - An OMG standard, closely related to UML, that enables metadata management and language definition.

Model - A formal specification of the function, structure and/or behavior of an application or system.

Model Driven Architecture (MDA) - An approach to IT system specification that separates the specification of functionality from the specification of the implementation of that functionality on a specific technology platform.

Normative – Provisions to which an implementation shall conform to in order to claim compliance with the standard (as opposed to non-normative or informative material, included only to assist in understanding the standard).

Normative Reference – References to documents that contain provisions to which an implementation shall conform to in order to claim compliance with the standard.

Platform - A set of subsystems/technologies that provide a coherent set of functionality through interfaces and specified usage patterns that any subsystem that depends on the platform can use without concern for the details of how the functionality provided by the platform is implemented.

Platform Independent Model (PIM) - A model of a subsystem that contains no information specific to the platform, or the technology that is used to realize it.

Platform Specific Model (PSM) - A model of a subsystem that includes information about the specific technology that is used in the realization of it on a specific platform, and hence possibly contains elements that are specific to the platform.

Request for Information (RFI) - A general request to industry, academia, and any other interested parties to submit information about a particular technology area to one of the OMG's Technology Committee subgroups.

Request for Proposal (RFP) - A document requesting OMG members to submit proposals to an OMG Technology Committee.

Task Force (TF) - The OMG Technology Committee subgroup responsible for issuing a RFP and evaluating submission(s).

Technology Committee (TC) - The body responsible for recommending technologies for adoption to the BoD. There are two TCs in OMG – the Platform TC (PTC) focuses on IT and modeling infrastructure related standards; while the Domain TC (DTC) focuses on domain specific standards.

Unified Modeling Language (UML) - An OMG standard language for specifying the structure and behavior of systems. The standard defines an abstract syntax and a graphical concrete syntax.

UML Profile - A standardized set of extensions and constraints that tailors UML to particular use.

XML Metadata Interchange (XMI) - An OMG standard that facilitates interchange of models via XML documents.