1. Project Name and ID

|  |  |
| --- | --- |
|  |  |
| **Positioning Security Risk Analysis standard within HL7** | Project ID:  |
|

|  |  |
| --- | --- |
| [ ]  | TSC Notification Informative/DSTU to Normative Date :  |

 |

1. Sponsoring Group(s) / Project Team

|  |  |
| --- | --- |
| Primary Sponsor/Work Group (**1 Mandatory**)  | **Project Services** |
| Co-sponsor Work Group(s) | (See list of consulting Work Groups under Domain Expert rep) |
|  |  |
| **Project Team:** |  |
| Project facilitator (**1** **Mandatory**) | **Project Services/Rick Haddorff, Freida Hall** |
| Other interested parties and their roles | TSC: John Quinn, Paul Knapp, Pat Van DykeHL7 Staff: Don Lloyd, Director of Technical Publications, Dave Hamill, Director HL7 Project Management Office |
| Multi-disciplinary project team (recommended) |  |
|  Modeling facilitator | n/a |
|  Publishing facilitator | n/a |
|  Vocabulary facilitator | n/a |
|  Domain expert rep | Consultation with: Security, Structured Docs, and Publishing Work Groups (WGs) |
|  Business requirement analyst | n/a |
|  Conformance facilitator (for IG projects) | n/a |
|  Other facilitators (SOA, SAIF) | n/a |
|  |  |
| Implementers **(2** **Mandatory** for DSTU projects): |
| 1) n/a |
| 2) n/a |

1. Project Definition
	1. Project Scope

|  |
| --- |
| This project will resolve potential security issues with implementation and/or executable artifacts produced by HL7 by early identification during the project scope definition and verifying security assessment is performed prior to publication. Updates to the project artifacts in subsequent projects may not require a new risk assessment with each updated publication, but an umbrella assessment for the standard or for a product family may be required. Note for reference only: [list of additional comments/questions from TSC](#_Notes_from_TSC) to be resolved during the project. |

* 1. Project Need

|  |
| --- |
| **The TSC chartered this project at the May 2014 WGM, discussed Saturday Q1 – Governance, TSC minutes posted at:** [**http://hl7tsc.org/wiki/index.php?title=2014-05-03\_TSC\_WGM\_Agenda**](http://hl7tsc.org/wiki/index.php?title=2014-05-03_TSC_WGM_Agenda) |

* 1. Success Criteria

|  |
| --- |
| **Project Scope Statement and Publication Request forms revised and rolled out to Co-Chairs** |

* 1. Project Objectives / Deliverables / Target Dates

|  |  |
| --- | --- |
|  | **Target Date**  |
| Project Services work with HL7 staff and TSC reps to create draft revisions to PSS and Publication Request supporting revisions described below: | **2014-06** |
| Make following changes to PSS:* Add checkbox to PSS to ask if project will be creating implementation or executable artifacts. See example below bulleted section for additional detail proposed.
* FAQ – this is informative, changing would not require change to scope statement. However, will require Security Risk Assessment prior to publication. Updates to the project artifacts in subsequent projects may not require a new risk assessment with each updated publication, but an umbrella assessment for the standard or for a product family may be required.
* Instructions: If project has implementation/executable deliverables will need to do a Security analysis prior to publication request.

Add new sub-section to Section 3**x.x Security Risk****Will this project produce executable deliverables?**

|  |  |
| --- | --- |
| [ ]  Yes | [ ]  No |

 | **TBD based on project completion but TSC does not want to hold up 2014 release – 2014 or 2014.1** |
| Make the following changes to Publication Request:* Add Interoperability Specification Matrix (ISM) to Publication Request
* Require projects to identify physical deliverables is a simple process such as check box and listing. Instructions to include example: executable, implementation artifact, (other TBD)

Ask follow on questions (TBD in collaboration from Structured Documents and Publishing) |  |
| Project Services/HL7 Staff to meet with identified Domain Expert Work Group to review proposed changes, solicit consensus on ISM stack for Publication Request | 2014-07 |
| Collect/confirm definitions for ISM artifactsLeverage [SAIF Artifact List](http://wiki.hl7.org/index.php?title=SAIF_Artifact_List) definitions http://wiki.hl7.org/index.php?title=SAIF\_Artifact\_List | 2014-07 |
| Submit final version PSS and Publication Request to TSC | 2014-08 |
| Verify appropriate guidance for Security Assessments available2014-06-27 update from Security WG, artifacts at: <http://wiki.hl7.org/index.php?title=Cookbook_for_Security_Considerations> | 2014-08 |
| HL7 Newsletter article  | January 2015 (missed September deadline) |
| Roll out new process at Co-Chair Dinner | 2014-09 WGM |
| eNews article | Following September WGM |
| Update Co-Chair Handbook and/or TSC wiki on new policy | Following September WGM |

* 1. Project Requirements

|  |
| --- |
| * Define new project scoping and publication requirements supporting a new TSC requirement defined during the May 2014 WGM to execute a Security Assessment for implementation or executable artifacts.
* Effective roll out of the new process to Work Groups.
 |

* 1. Project Risks

|  |  |
| --- | --- |
| Risk Description | **Since multiple stakeholders/Work Groups are involved the project may take longer than planned** |
| Impact Description | **Describe the impact of the risk.** |
| Probability: |

|  |  |  |
| --- | --- | --- |
| [ ]  High | [x]  Medium | [ ]  Low |

 | Severity: |

|  |  |  |
| --- | --- | --- |
| [ ]  High | [ ]  Medium | [ ]  Low |

 |
| Mitigation Plan | **Project Services will assess status bi-weekly and will attempt to keep project on schedule** |

|  |  |
| --- | --- |
| Risk Description | **Consensus on artifact definition and composition of the ISM stack may take longer than anticipated** |
| Impact Description | **Describe the impact of the risk.** |
| Probability: |

|  |  |  |
| --- | --- | --- |
| [ ]  High | [x]  Medium | [ ]  Low |

 | Severity: |

|  |  |  |
| --- | --- | --- |
| [ ]  High | [ ]  Medium | [ ]  Low |

 |
| Mitigation Plan | **Project Services will assess status bi-weekly and will attempt to keep project on schedule** |

|  |  |
| --- | --- |
| Risk Description | **Work Groups may need guidance on how to perform security assessment** |
| Impact Description | **Describe the impact of the risk.** |
| Probability: |

|  |  |  |
| --- | --- | --- |
| [x]  High | [ ]  Medium | [ ]  Low |

 | Severity: |

|  |  |  |
| --- | --- | --- |
| [ ]  High | [ ]  Medium | [ ]  Low |

 |
| Mitigation Plan | **Security Cookbook and related tutorial can assist; need to verify finalized versions are available** |

* 1. Project Dependencies

|  |
| --- |
| **Finalized Security Cookbook and Tutorial available** |

* 1. Project Document Repository Location

|  |
| --- |
| **Project Services GForge Documents:** <http://gforge.hl7.org/gf/project/psc/docman/Positioning%20Security%20Risk%20Analysis%20standard%20within%20HL7/> |

* 1. Backwards Compatibility

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Are the items being produced by this project backward compatible? | [ ]  Yes | [ ]  No | [ ]  Don’t Know | [x]  N/A |

 |

1. Products

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|

|  |  |
| --- | --- |
| [x]  | Non Product Project- (Educ. Marketing, Elec. Services, etc.) |

 |

|  |  |
| --- | --- |
| [ ]  | V3 Documents - Knowledge |

 |
|

|  |  |
| --- | --- |
| [ ]  | Arden Syntax |

 |

|  |  |
| --- | --- |
| [ ]  | V3 Foundation – RIM |

 |
|

|  |  |
| --- | --- |
| [ ]  | Clinical Context Object Workgroup (CCOW) |

 |

|  |  |
| --- | --- |
| [ ]  | V3 Foundation – Vocab Domains & Value Sets |

 |
|

|  |  |
| --- | --- |
| [ ]  | Domain Analysis Model (DAM) |

 |

|  |  |
| --- | --- |
| [ ]  | V3 Messages - Administrative |

 |
|

|  |  |
| --- | --- |
| [ ]  | Electronic Health Record (EHR) |

 |

|  |  |
| --- | --- |
| [ ]  | V3 Messages - Clinical |

 |
|

|  |  |
| --- | --- |
| [ ]  | Functional Profile  |

 |

|  |  |
| --- | --- |
| [ ]  | V3 Messages - Departmental |

 |
|

|  |  |
| --- | --- |
| [ ]  | V2 Messages – Administrative |

 |

|  |  |
| --- | --- |
| [ ]  | V3 Messages - Infrastructure |

 |
|

|  |  |
| --- | --- |
| [ ]  | V2 Messages - Clinical |

 |

|  |  |
| --- | --- |
| [ ]  | V3 Rules - GELLO |

 |
|

|  |  |
| --- | --- |
| [ ]  | V2 Messages - Departmental |

 |

|  |  |
| --- | --- |
| [ ]  | V3 Services – Java Services (ITS Work Group) |

 |
|

|  |  |
| --- | --- |
| [ ]  | V2 Messages – Infrastructure |

 |

|  |  |
| --- | --- |
| [ ]  | V3 Services – Web Services |

 |
|

|  |  |
| --- | --- |
| [ ]  | V3 Documents – Administrative (e.g. SPL) |

 |

|  |  |
| --- | --- |
| [ ]  | - New Product Definition - |

 |
|

|  |  |
| --- | --- |
| [ ]  | V3 Documents – Clinical (e.g. CDA) |

 |

|  |  |
| --- | --- |
| [x]  | - New/Modified HL7 Policy/Procedure/Process - |

 |

1. Project Intent (check all that apply)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |
| --- | --- |
| [ ]  | Create new standard |
| [ ]  | Revise current standard (see text box below) |
| [ ]  | Reaffirmation of a standard |
| [x] [ ]  | New/Modified HL7 Policy/Procedure/ProcessWithdraw an Informative Document |
| [ ]  | N/A (Project not directly related to an HL7 Standard) |

 |

|  |  |
| --- | --- |
| [ ]  | Supplement to a current standard |
| [ ]  | Implementation Guide (IG) will be created/modified |
| [ ]  | Project is adopting/endorsing an externally developed IG*(specify external organization in Sec. 6 below)* |
| [ ]  | Externally developed IG is to be Adopted |
| [ ]  | Externally developed IG is to be Endorsed |

 |

* 1. Ballot Type (check all that apply)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |
| --- | --- |
| [ ]  | Comment Only |
| [ ]  | Informative |
| [ ]  | DSTU to Normative |

 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|

|  |  |
| --- | --- |
| [ ]  | Normative (no DSTU) |
| [ ]  | Joint Ballot (with other SDOs or HL7 Work Groups) |
| [x]  | N/A (project won’t go through ballot) |

 |

 |

* 1. Joint Copyright

|  |  |  |
| --- | --- | --- |
|

|  |  |
| --- | --- |
| [ ]  | Joint Copyrighted Material will be produced |

 |

1. Project Approval Dates

|  |  |
| --- | --- |
| Sponsoring Group Approval Date | **2014-06-26** |
| Steering Division Approval Date 2014 May - PBS Metrics: Green2014 May Work Group Health: Green | **SD Approval Date CCYY-MM-DD** |

|  |  |  |  |
| --- | --- | --- | --- |
|

|  |  |  |
| --- | --- | --- |
| [PBS Metrics and Work Group Health Reviewed](http://gforge.hl7.org/gf/download/docmanfileversion/7241/10172/PBSMetricGuidanceforSDCoChairs2013Final.doc)? (required for SD Approval) | [ ]  Yes | [ ]  No |

 |

|  |  |
| --- | --- |
| Technical Steering Committee Approval Date | **TSC Approval Date CCYY-MM-DD** |
|

|  |  |  |
| --- | --- | --- |
| Joint Copyright Letter of Agreement received? (req'd for Joint Copyrighted material) | [ ]  Yes | [ ]  No |

 |

1. External Project Collaboration

|  |
| --- |
| **n/a** |

* 1. Stakeholders / Vendors / Providers

|  |  |  |
| --- | --- | --- |
| **Stakeholders** | **Vendors** | **Providers** |
| [ ]  Clinical and Public Health Laboratories | [ ]  Pharmaceutical | [ ]  Clinical and Public Health Laboratories |
| [ ]  Immunization Registries | [ ]  EHR, PHR | [ ]  Emergency Services |
| [ ]  Quality Reporting Agencies | [ ]  Equipment  | [ ]  Local and State Departments of Health |
| [ ]  Regulatory Agency | [ ]  Health Care IT | [ ]  Medical Imaging Service |
| [ ]  Standards Development Organizations (SDOs)  | [ ]  Clinical Decision Support Systems | [ ]  Healthcare Institutions (hospitals, long term care, home care, mental health) |
| [ ]  Payors  | [ ]  Lab | [ ]  Other (specify in text box below) |
| [ ]  Other (specify in text box below) | [ ]  HIS | [x]  N/A |
| [ ]  N/A | [ ]  Other (specify below) |  |
|  | [ ]  N/A |  |

* 1. Synchronization With Other SDOs / Profilers

|  |
| --- |
| Check all SDO / Profilers which your project deliverable(s) are associated with. |
| [ ]  ASC X12 | [ ]  CHA | [ ]  LOINC |
| [ ]  AHIP | [ ]  DICOM | [ ]  NCPDP |
| [ ]  ASTM | [ ]  GS1 | [ ]  NAACCR |
| [ ]  BioPharma Association (SAFE) | [ ]  IEEE | [ ]  Object Management Group (OMG) |
| [ ]  CEN/TC 251 | [ ]  IHE | [ ]  The Health Story Project |
| [ ]  CHCF | [ ]  IHTSDO | [ ]  WEDI |
| [ ]  CLSI | [ ]  ISO | [ ]  Other (specify below) |

1. Realm

|  |  |  |  |
| --- | --- | --- | --- |
|

|  |  |
| --- | --- |
| [ ]  | Universal |

 | [ ]  Realm Specific  |
|  | [ ]  Check here if this standard balloted or was previously approved as realm specific standard |

|  |  |
| --- | --- |
| [x]  | Not applicable |

1. Strategic Initiative Reference – For PMO/TSC Use Only

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| This section used only for Strategic Initiative Projects.

|  |  |
| --- | --- |
| [ ]  | 1. HL7 Recognition
 |
| [ ]  | 1. HL7 Internal Processes
 |
| [ ]  | 1. HL7 Implementation
 |

 |

### Notes from TSC members/discussion 6/9/2014 TSC call - TBD during the project:

* Which release, 2014 or 2014.1; don't want to hold up 2014 release
* Comments Re: PSS:

Did we want to limit this to a checkbox or also include an ISM matrix for them to indicate the artifacts which they though the project might produce as an aid to determining context and intent?

* + PV: I think this is a good question. It would keep SAIF in front of us a little earlier in the game. It does not mean that the item would not change---it would be a best guess.

Via email from Paul Knapp: Perhaps we should drop the term implementable in the question as standards are implementable. (resolved on 6/9 TSC call)

* Comments re: Roll out

If we can clearly identify the artifacts where the security concern may exist, then are you thinking that at publishing is where this question may be added (informally)? PV

* + Does this only apply to new projects, if not how to address existing projects
* Comment re: Project Dependencies:

Will the co-chairs be required to take the tutorial and will the tutorial take into consideration this ‘near miss’ for purposes of informing? PV Also, would it be free for co-chairs as incentive.