|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Title page | Date | Ed | Date is wrong on the draft distributed on 22 June | Change “Updated: 25 June 2014” to the correct date that the draft is uploaded and distributed. It should read “Updated: 22 June 2014”. |  |
|  | Title page | Abstract | Ed | Translates is the wrong term. | Change “engineers translates the seven” to “engineers transposes the seven”. |  |
|  | Title page | Citation format | Ed | The citation text needs correction | Change “Privacy by Design Documentation for Software Engineers (PbD-SE) Version 1.0, 25 June 2014, OASIS Working Draft 01, Revision 5, http://docs.oasis-open-org/…/pbd-se-v1 0-wd06.docx” to “Privacy by Design Documentation for Software Engineers (PbD-SE) Version 1.0, 22 June 2014, OASIS Working Draft 01, Revision 6, http://docs.oasis-open-org/…/pbd-se-v1 0-wd06.docx” |  |
|  | All pages | Page Footers | Ed | Date is wrong on the draft distributed on 22 June | Change the date in the footer to “22 June 2014”. |  |
|  | Introduction | FD6-FD18 | Ge | The introduction in an OASIS specification should introduce the specification, it purpose and scope, as well as indicate which sections are normative, if applicable. | Apply proposed changes in FD6-FD18 |  |
|  | Introduction |  | Te | The introduction is supposed to introduce the sections that are normative in the specification. | Add a new first paragraph to the introduction with the following text, “The normative sections in this specification are Section 2 and Section 3. Section 2, “Mapping of Privacy by Design Principles to Documentation” specifies the documentation needed to show evidence of support for each PbD principles. Section 3, “Conformance” specifies the conformance requirement of each of the documentation examples specified in section 2.” |  |
|  | Introduction | Paragraph 1 | Ed | Introduction should be specific about the specification. | Change “The OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) Technical Committee provides a specification to” to “This specification defines how to” |  |
|  | Introduction | Paragraph 1 | Te | “Software development process” is actually a system or set of processes and privacy & security should be integral to that. | Change “is a normal part of the software development process” to “should be integral to the software development process”. |  |
|  | Introduction | Paragraph 1 | Te | The point is that whether it is bug fixing, designing for security or designing for privacy, the later in the SDLC it is addressed the more costly it will be. Streamline the sentence to | Change “Given the savings that come from being proactive rather than trying to retrofit privacy into software, this specification streamlines the process of doing Privacy by Design and achieving cost savings.” to “As it has been shown to cost more, the later that a security vulnerability is found and corrected in the software development lifecycle (SDLC), taking a proactive approach to privacy will be more cost effective than reactively addressing privacy in the SDLC1. 1 ”Five steps to achieve success in your application security program”, IBM Whitepaper, http://searchsoftwarequality.bitpipe.com/detail/RES/1361993557\_566.html, 2012. |  |
|  | Introduction | Paragraph 2 | Ed | The better term might be “transpose” over use of translate. | Change “The PbD-SE specification translates the PbD principles to conformance requirements within software engineering tasks, and helps software development teams to produce artifacts as evidence of PbD-principle adherence.” to “This specification transposes the PbD principles into activities within the software engineering that helps software development teams to produce artifacts that serve as evidence of adherence to the PbD principles.” |  |
|  | Introduction | Paragraph 2 | Te | The sentence should focus on the benefit of conforming to the specification. | Change “Following the specification facilitates documentation of privacy requirements from software conception to retirement, thereby providing a plan around adherence to or compliance with Privacy by Design principles, and other guidance to privacy best practices, such as NIST’s 800-53 Appendix J [NIST 800-53] and the Fair Information Practice Principles (FIPPs)” to “Conformance to the specification will facilitate documenting implementation of privacy requirements throughout the SDLC, from concepting to termination of the project.” |  |
|  | Introduction | Paragraph 2 | Ed | There is no reason to have the reference to PMRM in this paragraph. | Remove “[PMRM-1.0]”. |  |
|  | Introduction | Paragraph 2 | Te | This specification is not a part of and not intended to be associated with an auditing framework, such as the role that ISO 27001 serves as a framework for information security management system and the foundation for information security systems auditing. The specification is not intended as a privacy management system. | Change “may use the PbD-SE methodology for documenting and auditing such adherence to *Privacy by Design* throughout the entire software development life cycle.” to “will find the specification useful for documenting implementation of PbD throughout the SDLC.” |  |
|  | Introduction | Paragraph 2, Last sentence | Te | It is unclear to an engineer, without privacy legal counsel, if application of this specification will “serve as evidence of compliance” to privacy regulations. The sentence must be toned down to reflect the role the specification serves in reducing overall privacy risk and documentation of best practices. | Change “Correct application of PbD principles to software engineering helps lower overall risk, and may serve as evidence of compliance with privacy law and regulation.” to “Application of the specification should facilitate lowering overall product privacy risk and serve to demonstrate steps taken to address privacy, as it relates to PbD principles.” |  |
|  | Introduction | Paragraph 3, 1st Sentence | Te | The first sentence is not needed. | Delete first sentence. |  |
|  | Introduction | Paragraph 3 | Te | The rest of Paragraph 3 needs to be rewritten to introduce the integral importance of the Annex to the specification. | Change “The PbD-SE specification (and its “Annex to the Privacy by Design Documentation for Software Engineers” guide) helps engineers to visualize, model, and document PbD requirements and embed the principles within software engineering tasks. It also helps inform those organizational governance processes that oversee the software engineers.” to “This specification is complemented by an Annex that provides guidance on how to model, visualize and document PbD requirements and embed controls that support PbD principles within software deliverables. The Annex also helps identify organizational governance and processes that relate to software engineering.” |  |
|  | Introduction | Paragraph 4 | Te | This paragraph adds nothing to the introduction of the specification. | Delete this paragraph. |  |
|  | Introduction | Paragraph 5 | Te | This paragraph adds nothing to the introduction of the specification. However, the paragraph content related to not mandating a specific format for documentation of data flow, use cases, etc. is coupled to Paragraph 3 and should be inserted as a sentence at the end of that paragraph. | Delete this paragraph and add the following to the end of paragraph 3, “This templates and examples for use case, data flow diagrams, spreadsheet data classification and other documentation are intended as references to best practices. The specification does not mandate a particular format but instead includes in the Annex illustrative types of artifacts that should be generated in the various stages of the SDLC. |  |
|  | 1.1 Context and Rationale |  | Te | This section is not a normal section in an OASIS specification. The content is rhetorical and does not contain any specification content. The specification is intact without this section. | Delete this section. |  |
|  | 1.2 Objectives |  | Te | This section is not a normal section in an OASIS specification. However, the content is very applicable to the function of the Introduction. The last sentence of Section 1.2 Objectives speaks to future work and is not needed in the specification. | Delete this section and move the content to new paragraph 4 of the introduction. However, delete the last sentence of section 1.2 Objectives. |  |
|  | 1.3 Intended Audience |  | Te | The current text is too long, complexly worded. A terse, simplification of the intended audience and benefits of the specification is needed. | Replace the text in section 1.3 with, “This specification is intended for use by software engineers that desire to understand how to integrate PbD into software engineering and their PDLC. The specification is also intended for use by management of software engineering product programs that desire to assure that their programs reflect best practices in documenting PbD principles have been followed. The specification is also intended for use by management of organizations that desire that their organization governance and business processes reflect an accountable organization, intending to be compliant with privacy laws and regulations. This specification is also intended for privacy officers, compliance officers and internal auditors that desire to understand best practices in providing evidence of following PbD principles. In addition, other OASIS TCs and standards bodies may find the PbD-SE specification useful in producing evidence of adherence to and/or compliance with PbD principles.” |  |
|  | 1.4 Outline of the Specification | Paragraph 1, list 1 | Te | The 3rd and 4th list items are not contained in the specification, proper. | Delete the 3rd and 4th list items. |  |
|  | 1.5 Terminology |  | Te | Architectural Principle is not a term used in the document. | Delete the term. |  |
|  | 1.5 Terminology |  | Te | Information Privacy is not a term used in the document. | Delete the term. |  |
|  | 1.5 Terminology |  | Te | Personal Information is only used in section 1.1. If disposition of FD19 is ACCEPT then this term will not be used in the document. | Delete the term. |  |
|  | 1.5 Terminology |  | Te | Software Organizations is not the only organizational type that this specification is intended for. It is too limiting to focus just on software organizations. Many types of organizations create and make use of software and are potential intended readers of the specification. | Delete the term and change every occurrence in the specification of the term “software organization” to “organization”. |  |
|  | 1.6 Normative References |  | Te | PMRM-1.0 is not a normative reference to the normative sections of the specification (IE, section 2 and 3). | Move the reference to section 1.7 “Non-Normative References”. |  |
|  | 1.7 Non-Normative References |  | Te | NIST 800-53 is not a necessary reference to either the normative or non-normative sections of the document. | Delete the reference. |  |
|  | 2 Mapping of Privacy by Design Principles to Documentation |  | Te | This section would benefit by an initial paragraph that explained the rational for the mapping of PbD principles to documentation. | Add the following text as a paragraph to section 2, “Applying PbD to software engineering begins with an understanding of the 7 Foundation Principles of PbD [Cavoukian 2011]. These foundation principles are supported by a set of sub-principles. The principles are by nature subjective. However, software engineering is based on objective and measurable set of activities and tasks. Mapping the PbD principles to supporting documents provides evidence that these privacy requirements have been addressed.” |  |
|  | 2 Mapping of Privacy by Design Principles to Documentation | Paragraph 1 | Ed | Conformance term is not appropriate in the context of paragraph. | Replace the text of paragraph 1 with, “Table 2.1 provides a mapping between the seven PbD principles and the supporting sub-principles and the required implementation evidence.” |  |
|  | Table 2.1 |  | Ed | It will be difficult to reference each of the documentation items when completing a conformance review. | Add numeric (EG, (1), (2), (3)…) prefixes to each of the documentation requirements. |  |
|  | Table 2.1 |  | Te | The normative terms in Table 2.1 (IE, SHALL) is inappropriate for this table. Conformance terms for each documentation items are addressed in section 3 and Table 3.1. Having the conformance terms in both places will lead to possible conflicting specification of conformance terms between the two tables. | Delete the conformance terms from the documentation item definitions in column 3 of Table 2.1. |  |
|  | Table 2.1 | Row 1 | Te | The documentation requirement “SHALL include privacy risk/threat model(s) including analysis and risk identification, risk prioritization, and controls clearly mapped to risks” should be broken into components associated with documenting the risk management framework used by the organization, the organizational risk aspiration or vision and the product specific risk impact assessment report. | Change the text “SHALL include privacy risk/threat model(s) including analysis and risk identification, risk prioritization, and controls clearly mapped to risks” to “Document the risk management framework adopted by the organization.” “Document the quantitative risk intent of the organization.” “Document the risk impact assessment report for the product.” |  |
|  | Table 2.1 | Row 3 | Te | The Introduction of the specification is clear that no template or format is mandated for documenting evidence supporting PbD implementation. However, column 3 includes “SHALL use the OASIS PbD-SE Privacy Use Template (see PbD-SE Annex Section 5 [PbD-SE-Annex-1.0]) or the more comprehensive OASIS PMRM methodology [PMRM 1.0] or equivalent for identifying and documenting privacy requirements.” | Change the text to, “document use case, data flows, data classification, lists of privacy controls, risk assessment results, privacy requirements using best practices, such as those documented in [PbD-SE-Annex-1.0]”. |  |
|  | Table 2.1 | Row 3 | Te | “SHALL include human sign-offs/privacy checklists for software engineering artifacts” is less than clear on the intended documentation. My assumption is that this requirement is to have evidence from a privacy professional that the specified privacy requirements have been implemented by the software engineering team, prior to “Go-Live” of the product. | Change the text to read “Documentation of privacy assessment sign-off by individual accountable for organization’s privacy program”. |  |
|  | Table 2.1 | Row 3 | Te | “SHALL include privacy review reports (either in reviewed documents or in separate report)” is overtly prescriptive and not helpful for documenting the intended purpose. | Change the text to read, “Document privacy review findings.” “Document security review findings.” “Provide sign-off of implementation of privacy review findings by privacy accountable software engineer.” “Provide sign-off of implementation of security review findings by security accountable software engineer.” |  |
|  | Table 2.1 | Row 5 | Ed | The text “SHALL demonstrate designs and implementations that satisfy state-of-the-art privacy properties” is subjective and hard to assess conformance. Rewording is needed. | Reword to “Document how privacy and security industry best practices for feature concepting, design, implementation, operational support have been followed”. |  |
|  | Table 2.1 | Row 3 | Te | The following list of document requirements need to be reviewed, “SHALL use the OASIS PbD-SE Privacy Use Template (see PbD-SE Annex Section 5 [PbD-SE-Annex-1.0]) or the more comprehensive OASIS PMRM methodology [PMRM 1.0] or equivalent for identifying and documenting privacy requirements.  SHALL contain description of its business model showing traceability of personal data flows for any data collected through new software services under development.  SHALL include identification of privacy design principles  SHALL contain a privacy architecture  SHALL describe privacy UI/UX design”. These document requirements are not sufficiently aligned with their underlying necessity. | Change these document requirements to “Document primary use cases for the product.” “Document applicable privacy principles, requirements.” “Document the inventory and classification of all personal data collected and processed such that all interactors, data flows, security & privacy classification, purposes, security measure for transfers, cross-border transfers, server locations, retention/deletion plan is clearly identified.” “Document the threat assessment results, including planned mitigations and residual vulnerabilities.” “Document privacy design patterns, privacy enabling technology integrated into the product.” |  |
|  | Table 2.1 | Row 3 | Te | is most effective if the metrics are consistent across the organization and reported on a periodic basis to the organization’s management team. | The document requirement “SHALL define privacy and security metrics” should be moved from “3. Privacy Embedded into Design” to “1. Proactive not Reactive; Preventative not Remedial”. |  |
|  | Table 2.1 | Row 3 | Te | The list of documentation requirements do not address security requirements. Since you cannot have privacy without adequate security, additional document requirements for assuring adequate address of product security best practices is needed. | Add the following documentation requirements to column 3 of row 3 “Privacy embedded into design”, “Document security code review requirements, process and results.”, “Provide sign-off by security responsible software engineer that no identified vulnerabilities are remain unmitigated.” “Document security scans have been regularly conducted on all server environments.” “Provide sign-off by security responsible software engineer that no issues identified by scans remain unmitigated.” “Document system hardening steps taken on application and server components.” “Provide sign-off by security responsible engineer that hardening steps have been taken.” “Document the security requirements for 3rd party partners.” “Provide sign-off by legal responsible that all 3rd party partner contracts include reference to 3rd party security requirements and data protection requirements required of 3rd parties processing personal data.” |  |
|  | Table 2.1 | Row 3 | Te | Administrative access control needs to be in-place and documented for access to administrative functionality when PII, especially sensitive PII is processed. Individual accounts must be used instead of group accounts. Administrative access to the system must be given only for persons that have legitimate reason. Level of access rights must be set according to the role/task, with least-privileges philosophy.  . | Add documentation requirement for “Document access control for systems that have administrative functions, when PII, especially sensitive PII is process.” “Provide sign-off by security responsible software engineer that access control requirements implemented and tested.” |  |
|  | Table 2.1 | Row 3 | Te | There need to be documentation that logging systems for the product have been reviewed to minimize any log records with PII, for cases where there are no legitimate purposes for collecting the PII. | Add documentation requirement for “Document that audit logging is enabled for key activities of the product.” “Document the log record elements have no PII, unless there is legitimate purpose and that there is a retention/deletion.” |  |
|  | Table 2.1 | Row 5 | Te | In 5 “End-to-end Lifecycle Protection”, the list of documentation does not include business continuity and recovery support. | Add the following documentation requirements to column 3 of row 5 “End-to-end Lifecycle Protection”, “Document tested plan for business continuity, recovery of the product for time of emergency, major incident, crisis, such that product is restored and maintained, including key staff, resources, services, architecture and actions.” “Document the staffed and resourced reactive incident response plan to manage reactive security, incident response, security related monitoring and upgrading in emergency situations.” |  |
|  | Table in Section 3 |  | Ed | The conformance section is a table. But there is not table title. | Add “Table 3.1 – Conformance” to the top of the table in section 3. |  |
|  | Section 3 | Paragraph 1 | Ed | This section summarizes the requirements for meeting the PbD “Conformance Targets” of this specification. | Change the text to “Software engineering teams, management teams, organizations that desire to conform to this specification SHALL demonstrate evidence of implementing all the mandatory documentation requirements listed in Table 3.1 with a “SHALL” conformance term. In addition, they SHALL demonstrate evidence of implementing all the recommended documentation requirements listed in Table 3.1 with a “SHOULD” conformance term, unless they can provide evidence of why this conformance requirement is not applicable to them. |  |
|  | Section 3 | Table 3.1 | Te | Assessing conformance to the specification will be difficult without having precise, unique identification of each conformance requirement. See FD31. | Table 3.1 needs to reference the unique identifier for each associated documentation requirement. |  |
|  | Section 3 | Table 3.1, 3. Privacy Embedded into Design | Te | “3 c) SHALL include identification of privacy design principles” does not make sense for being “SHALL” conformance level. It is sufficient that privacy requirements for the product are mandatory. | Change conformance term to “SHOULD”. |  |
|  | Section 3 | Table 3.1, 3. Privacy Embedded into Design | Te | “3 d) SHALL contain a privacy architecture” does not make sense for being “SHALL” conformance level. Comprehensive privacy architectures are no pervasive across the ICT industry. The technology maturity is only at level of Privacy Enabling Technologies. | Change conformance term to “SHOULD”. |  |
|  | Section 3 | Table 3.1 3. Privacy Embedded into Design | Te | “3 e) SHALL describe privacy UI/UX design” does not make sense for being “SHALL” conformance level. What makes sense is to have end user privacy control features documented. In addition, having test cases to assure that the end user privacy controls are implemented, might make sense. | Change document requirements to “Document end user privacy controls.” “Document test cases to verify end user privacy controls are functional.” The conformance requirement for the two requirements is “SHOULD”. |  |
|  | Section 3 | Table 3.1 3. Privacy Embedded into Design | Te | “i) SHALL treat privacy-as-a-functional requirement i.e. functional software requirements and privacy requirements should be considered together, with no loss of functionality.” is a problematic documentation requirement. Privacy requirements can only be listed as a functional requirements if there are clear subjective methods to implement the requirement. So privacy requirements have less mature controls that are anything but functional and instead are non-functional requirements. For example, having privacy accountable software engineer provide sign-off documentation that a requirement has been met is not a functional requirement. | Delete this documentation requirement from Table 2.1 and Table in Section 3. |  |
|  | Section 3 | Table 3.1 3. Privacy Embedded into Design | Te | “k) SHALL be produced for all stages of the software development lifecycle from referencing applicable principles, policies, and regulations to defining privacy requirements, to design, implementation, maintenance, and retirement.” Is an ackwardly phrased requirement and it is not clear how this requirement is to be met. | Delete this documentation requirement from Table 2.1 and Table in Section 3. |  |