Tech Semantic

Data Privacy Risk Impact Assessment

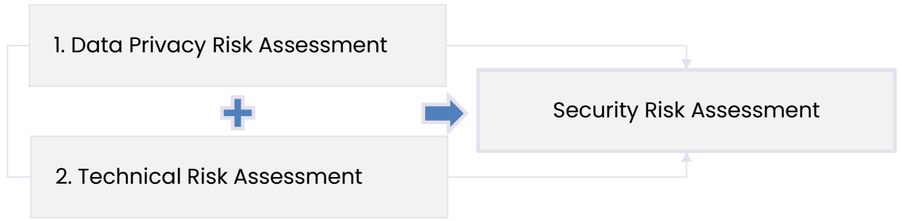
[Part I : Security Risk Assessment Process]

Area : Needs Analysis

- Sample document only.
- Contains masked and redacted information.
- Conceptual and may not suit all uses.

Author : Delon Xavier | Contact : +61 432 043 705
Email : delon.xavier@techsemantic.com | https://www.delonxavier.com

1. Context



A security risk assessment aims to identify, evaluate, and prioritize potential security risks within an organization's infrastructure, systems, and processes. This assessment helps in understanding vulnerabilities that could lead to unauthorized access, data breaches, or operational disruptions across two high impact functional areas.

- Data Privacy Risk Assessment
- Technical Risk Assessment

Outcomes :

It supports the development of a robust security posture, ensuring the protection of critical assets, maintaining business continuity, and complying with industry standards and regulations.

Data Privacy Risk Assessment

Key Objective :

- The objective of a data privacy risk assessment is to evaluate the potential risks to the privacy and security of personal and sensitive data within an organization's projects.
- The process aims at introducing checkpoints in the current system to allow assess, recommend and implement appropriate safeguards, policies, and procedures to mitigate risks, enhancing the organization's ability to protect privacy rights.

Key Outcomes :

- Outcomes of a data privacy risk assessment include identifying high-risk data processing activities, establishing privacy controls, assessing the adequacy of current data protection measures, and recommending strategies for mitigation.

2. Introduction to Data Privacy & Compliance

Implementing a data privacy risk assessment process early in a project lifecycle is critical for ensuring compliance across data privacy related regulations laid down by Office of the Australian Information Commissioner (OIAC)

OIAC, through the Privacy Act 1988 and the Australian Privacy Principles (APPs) govern the handling of personal information by Australian government agencies, private sector organizations, and certain other entities.

Key guidelines :

1 Data Inventory & Classification

- Data Mapping : Identify types of personal data collected, stored, processed and shared across the organisation.
- Data Classification : Categorise data according to its sensitivity.
- Data Flow : Understand how data will move across the organisation (from collection to deletion – based on retention policies / rules)

2 Compliance with Regulations

- Global Compliance : Ensure alignment with local, national and international data privacy laws, as applicable (APPs, GDPR, HIPAA and others)
- Privacy by Design : Incorporate privacy considerations into business processes and systems from the outset.
- Data Subject Rights : Enable and monitor processes that respect the rights of individuals (right to access, erasure, data portability)

2. Introduction to Data Privacy & Compliance

3 Risk Identification & Assessment

- Risk Assessment : Evaluate risks to personal data from internal and external sources.
- Threats & Vulnerabilities : Assess potential threats like cyber attacks, human error or vendor risks related to systems and processes.
- Privacy Impact Assessment : Conduct PIAs when introducing new projects or technologies that involve the processing of personal data.

4 Data Protection & Security Measures

- Data Minimization : Ensure only necessary data is collected and processed.
- Data Security : Use encryption, anonymization & pseudonymization to protect sensitive data.
- Access Control : Implement role-based access controls (RBAC) ensuring only authorised personnel can access personal data.

5 Third-party Management

- Vendor Risk Management : Assess risks posed by third-party vendors who may have access to personal data.
- Contractual Obligations : Ensure that third-party contracts contain adequate privacy and data protection clauses related to data processing.
- Due Diligence : Perform due diligence on third-parties, including security audits and privacy assessments.

2. Introduction to Data Privacy & Compliance

6	Incident Management & Response

Incidence Response	: Define a process for data privacy incidents (breaches, leaks etc)
Breach Notifications	: Define process for notifying regulators and effected individuals within defined time limits, if any.
Post Incident Review	: After an incident, perform root cause analysis, remediate vulnerabilities and adapt to risk management strategies to prevent future incidents.

7	Continuous Improvement

Feedback Loop	: Regularly review risk management process to adapt to evolving business processes, new tech adoption and new legal requirements.
Periodic Audits	: Review current systems changes in design, assess and manage related data privacy risks.
Lessons Learnt	: Implement lessons learnt from incidents and audits to improve organisations posture towards data privacy risks.

3. Data Privacy Risk Assessment (DPRA) - Proposed Process

› Elements

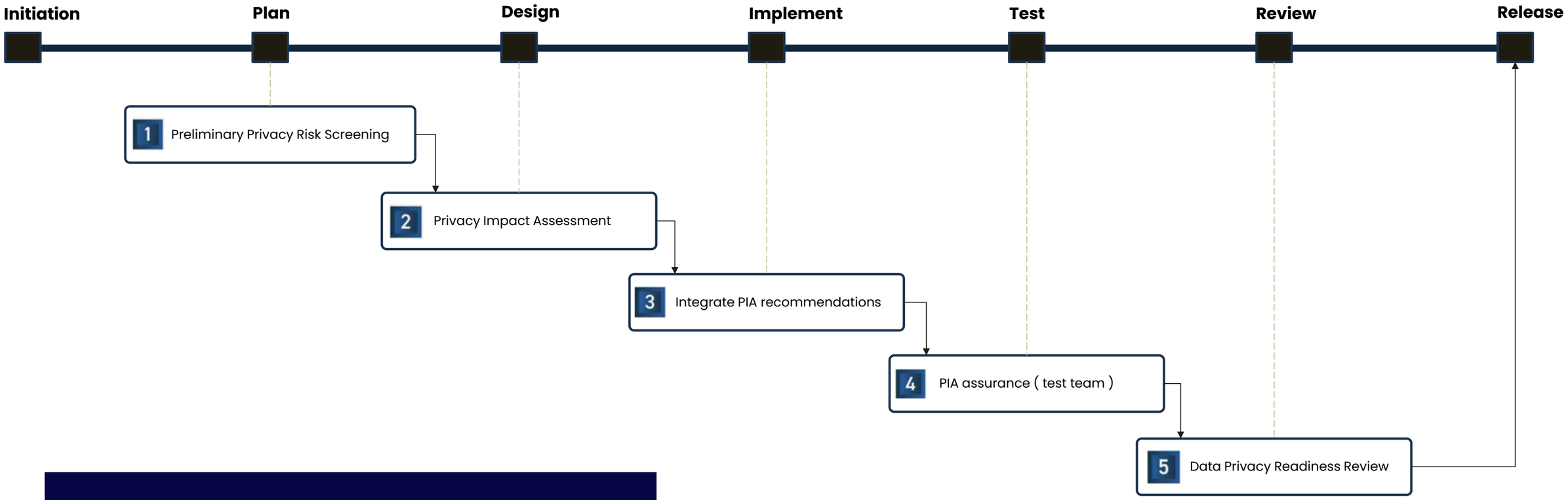
1. The **preliminary privacy risk screening (PPRS)** is an initial assessment aimed at identifying whether a project needs to undergo a formal privacy impact assessment based on high level data privacy checklist items.

2. **Privacy impact assessment** is a detailed exercise to identify data privacy related risks & impacts being carried by a project and recommends mitigation strategies to be carried out as part of project go live entry criteria. Privacy risks are added to risk register and planned risk actions agreed.

3. **Integrate PIA recommendations** is to be considered as project deliverables, and thus must be incorporated within project requirements. This may also include requirements related to project transition to BAU / Ops.

4. **PIA assurance** involves data privacy related requirements to be tested as part of project test scope, included in project UAT exit criteria.
This may also involve updating risk register providing inputs for data privacy readiness review.

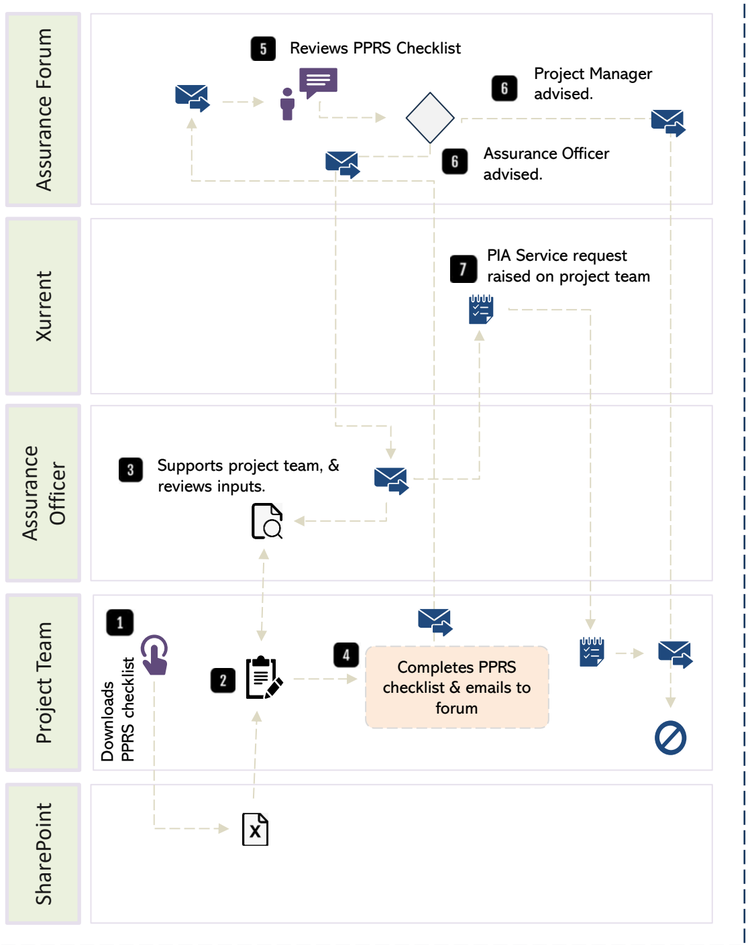
5. **Data privacy readiness review** is a formal joint collaborative effort to be conducted by projects and assurance teams validating all recommendations have been provisioned as part of project and/or transition scope including review of known & residual risks related to data privacy.



1 Preliminary Privacy Risk Screening [PPRS]

Project Manager | Project Team | Assurance Officer | Assurance Forum

SharePoint | Xurrent | PPRS Checklist | PIA Service Request



1. Project Manager downloads the PPRS checklist from SharePoint.
2. Project team completes the requested details via the checklist.
3. Assurance officer supports project team, review details and advise when complete.
4. On completion, PPRS checklist is sent to mentioned email (data assurance forum for review)
5. Assurance forum reviews project PPRS checklist details and request clarification from assurance officer or project manager as needed.
6. Forum advises Project Manager and Assurance officer on outcome.
   - If PIA NOT required, email is sent to all parties and PPRS process completed.
   - If PIA is required, email is sent to all parties and assurance officer is advised to raise PIA service request on project team.
7. PIA service request is raised by Assurance Officer on project team.
   - Email carrying service request details sent to project team.
   - PIA service request is open till PIA process is completed.
   - PPRS process completed.

Preliminary Privacy Risk Screening Checklist

The introduction of a PPRS checklist is an attempt to systemise the decisioning whether a project qualifies for further assessment via a formal privacy impact assessment.

Key elements :

1. Project Details
- Project Overview & Charter
- List of stakeholder involved and key contacts for data privacy assessment.

2. Data Involvement
- Will the project involve the collection, use, or processing of personal data?
- Does the project involve sensitive personal data (e.g., health data, financial information)?

3. Data Subjects
- Will the project impact individuals' privacy (e.g., customers, employees, users)?
- Are data subjects located in multiple regions or jurisdictions (e.g., cross-state data)?

4. Purpose of Data Use
- Is the processing of personal data essential to the project?
- Is the purpose of the data processing clearly defined?

5. Data Sharing and Access
- Will personal data be shared with third parties or external vendors?

6. Security Considerations
- Are there any early plans for securing personal data (e.g., encryption, access controls)?

7. Data Retention
- Will personal data be retained beyond the duration of the project?

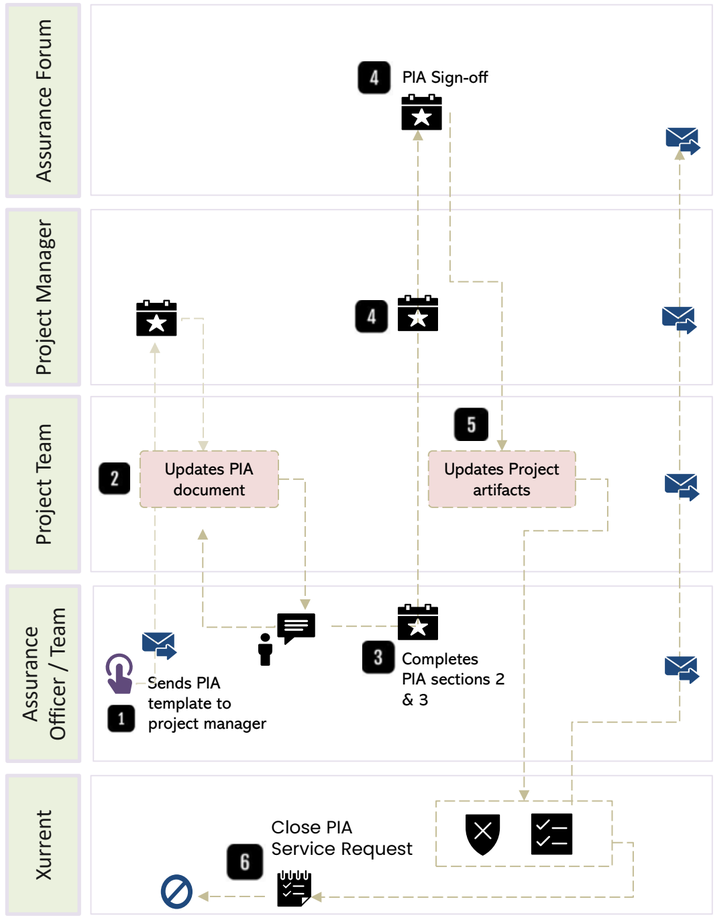
8. Regulatory Compliance
- Does the project need to comply with any data protection regulations (e.g., GDPR, CCPA)?

9. Privacy Risks
- Are there any known privacy concerns or potential risks associated with the project?

2 Privacy Impact Assessment [PIA]

Project Manager | Project Team | Assurance Officer | Assurance Forum

PIA Template | Risk Register | Planned actions | PIA Service Request



1. Assurance officer sends the PIA template to the Project Manager.
2. Project Manager gets the project team to provide PIA details (supported by assurance team)
3. Assurance officer completes section 2 and 3 – discusses and consensus arrived across assurance and projects.
4. Assurance forum is onboarded by the project manager & assurance officer and sign-off is obtained.
5. Project team updates project artifacts – namely privacy risk register and planned actions log.
   - Manager informs all groups that project artifacts reflects PIA.
6. Project manager closes PIA Service Request.

Privacy Impact Assessment (PIA)

PIA Is a process to evaluate the potential impact of a project or system on personal privacy. It helps identify and mitigate privacy risks through risk response planning & action.

Key elements :

1. PIA Inputs

- Project overview, objectives, scope, outcomes and key stakeholders.
- List of privacy information types, how information will be used and disclosed.
- List of 3rd party, their roles and extent of their working with privacy data.
- Depiction of personal information flows.

2. Privacy Impact Analysis

- Identifies and critically analyses how the project impacts on privacy, both positively and negatively.

3. Compliance against Australian Privacy Principles

- In this section, the organisation assesses how its practices align with the 13 Australian privacy principles.
- Also identifies areas where improvements may be needed to ensure privacy compliance.

Privacy Risk Register

- All identified risks are logged with probability, impact, risk rating along with risk mitigation strategy including residual risks & its rating.
- Each risk is assigned an owner who shall be responsible to drive the risk mitigation strategy.

Privacy Risk Actions Log

- Planned risk response actions are logged into an actions register for progress tracking.

4. PIA Sign-off

- PIA is signed off by Project Manager and Assurance Forum representatives.

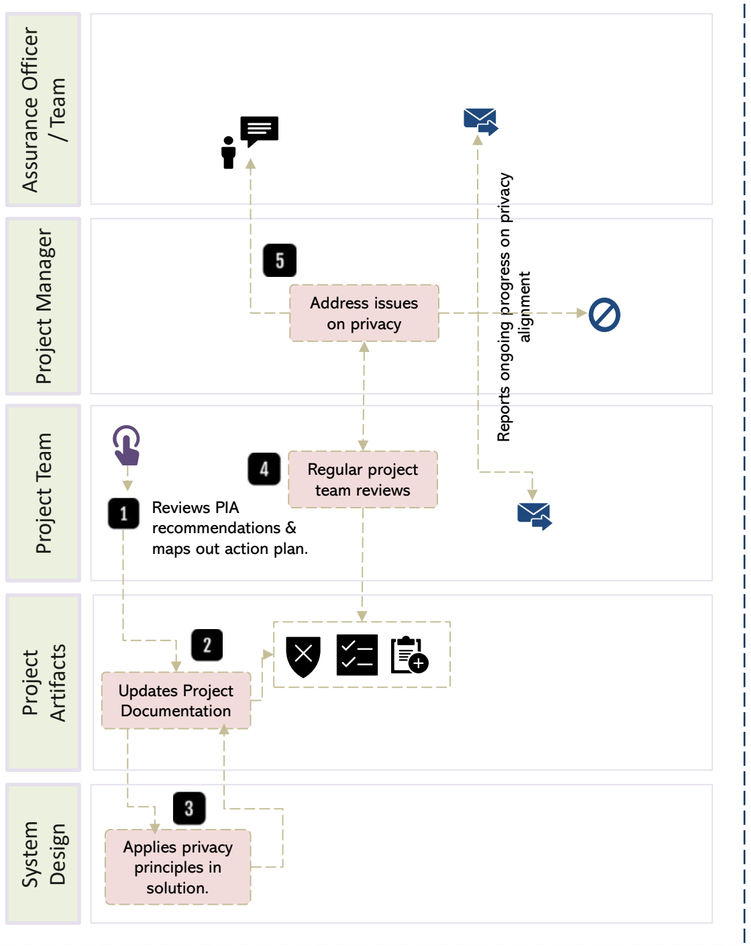
5. Update project artifacts

- Project privacy risk register and privacy risk actions log is updated to reflect PIA details.

3 Integrate PIA recommendations.

Project Manager | Project Team | Assurance Officer

PIA Template | Risk Register | Planned Actions Log | Project Requirements



1. Project reviews PIA measures & recommendations including prioritisation of actions.
2. Updates project artifacts to reflect plan of action.
3. Incorporates privacy measures into solution design with ongoing updates to project artifacts.
4. Regular reviews are conducted to track progress of privacy measures into system design & development.
5. Project Manager addresses privacy issues across the project team as needed via the assurance officer / team.

   Regular updates on progress sent to various stakeholder groups as per communication plan.

Integrate PIA recommendations & actions into project design

Integrating PIA recommendations into design ensures project deliverables comply with privacy expectations and reduces potential risks.

Key elements :

1. Initial review and understanding of PIA recommendations.

- Thoroughly review privacy measures and recommendations.
- Prioritise items based on impact, feasibility and alignment with overall goals.
- Update privacy risk register & planned actions log as per agreed priority.

2. Integration into project scope, stakeholder requirements and project plan

- Map the PIA recommendations into project deliverables (includes transition to BAU deliverables) including its back traceability to risk register and planned actions log.
- Modify project timelines, budgets and resource allocations, as necessary.
- Update project artifacts to maintain currency.

3. Implement privacy measures

- Apply privacy by design principles in the system architecture & solution design.
- Conduct regular reviews to verify privacy implementation meets the plan. .

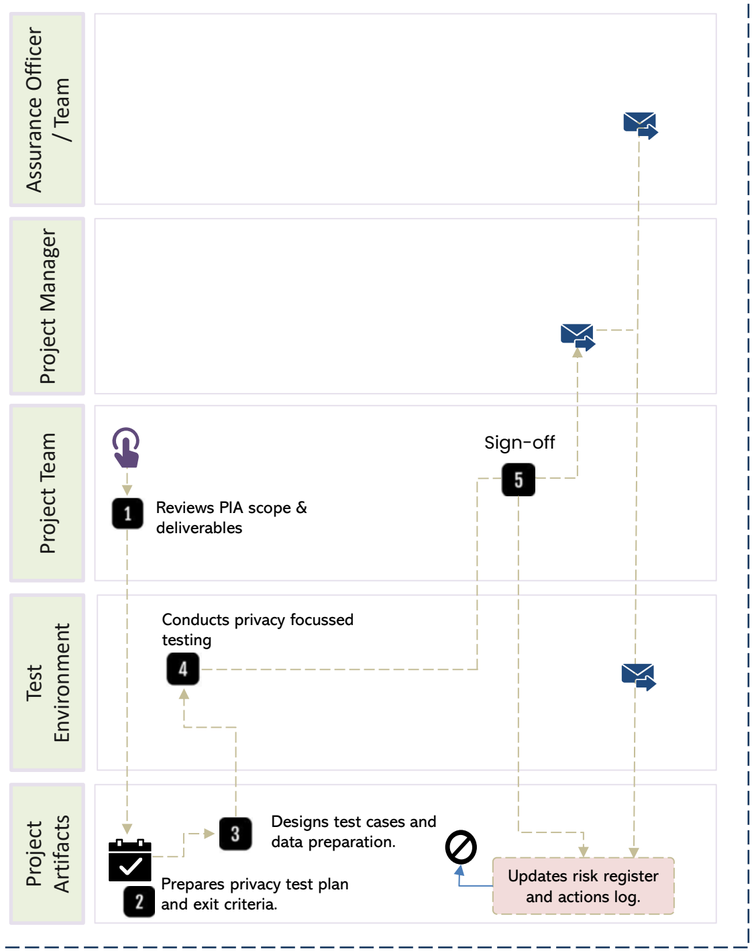
4. Collaborative risk management & communication

- Maintain ongoing assessment of projects privacy risk exposure & compliance as system development makes progress.
- Establish clear communication channels to report ongoing progress and address issues on privacy alignment.

4 PIA Assurance (Test Team)

Project Manager | Project Team | Assurance Officer | Assurance Forum

Risk Register | Planned Actions | Privacy Test Inputs / Outputs



1. Project team reviews privacy scope and deliverables for system testing.
2. Prepares a privacy test plan including test data requirements and privacy test exit criteria.
3. Project team defines privacy test cases and related test data required to meet exit criteria.
4. Project team implement privacy testing in SIT & UAT including regression testing until exit criteria is reached.
5. Once exit criteria is arrived at, project manager updates risk register and planned actions log.
   - initiates data privacy sign-off across project team and assurance team.

PIA Assurance

Ensure project deliverables meet the required Australian privacy principles, standards and defined specifications.

Key elements :

1. Review privacy scope and deliverables for system testing.

- Thoroughly review of privacy related requirements including PIA and internal policies to get a clear understanding o privacy goals, data minimization, access controls, data retention and anonymization requirements.

2. Develop a privacy test plan.

- Create the plan to outline specific privacy use cases including tools & test data requirements.
- Include entry and exit criteria including sign-off criteria related to privacy compliance.

3. Implement privacy specific test cases and test data.

- Design test cases and supporting test data to cover data encryption, role-based access control, data minimization, anonymization / pseudonymization, data retention & deletion.

4. Conduct privacy focused security testing.

- Check for privacy by design and privacy by default principles are applied.
- Document & review test results including regression testing activities.

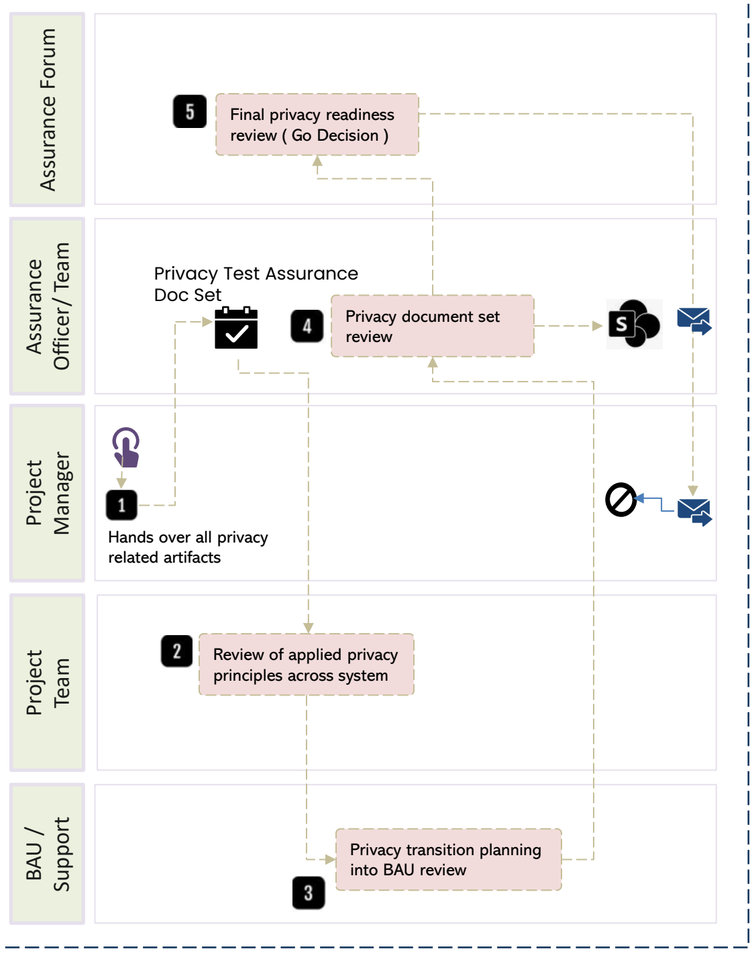
5. Sign-off on privacy related deliverables.

- Ensure privacy acceptance testing is signed-off and updates made to risk register and planned actions log.

5 Data Privacy Readiness Review

Project Manager | Project Team | Assurance Officer | Assurance Forum

Risk Register | Planned Actions | Privacy Test Assurance Doc Set



1. Project Manager hands over privacy related artifacts to assurance officer.
2. Assurance Officer reviews applied privacy principles across system design.
3. Assurance Officer will review privacy transition planning to BAU.
4. Privacy Officer will review all privacy related document sets handed over by project manager and uploaded to SharePoint.
5. Final privacy readiness review by assurance forum and GIO decision reached.

Data Privacy Readiness Review.

Ensures data privacy related requirements & controls have been provisioned for, including updates made into the risk register and risk actions log.

Key elements :

1. Privacy assurance handover.

- Provide the following documents…
- Privacy test completion criteria including test summary report,
- Privacy test results & open defects if any (low priority),
- Updated privacy risk register & planned actions log,
- Stakeholder sign-off

2. Final review of applied privacy principles across system design (before go live)

- Privacy by design, user consents, data minimization, handling and storage.
- Role based access controls.
- Data anonymization, pseudonymization, retention and deletion policies applied

3. Transitioning planning for privacy design into BAU

- Training & awareness across required touchpoints.
- Incident report & breach notification process in place.
- Privacy documentation review.

4. Privacy document sets final review

- Privacy readiness artifacts reviewed and uploaded to SharePoint (assurance team directory)

5. Data Privacy Readiness Go live

- Final review by assurance forum and privacy readiness go decision provided.

4. Data Privacy Document Sets

#	Stage	#	Document		Notes
1.	Preliminary Privacy Risk Screening (PPRS)	1.01	Preliminary Privacy Risk Screening Checklist		
2.	Privacy Impact Assessment (PIA)	2.01	Completed PPRS Checklist		
		2.02	Company Privacy Policies and Security Pack		
		2.03	Completed PIA document		
		2.04	Privacy Risk Register		
		2.05	Privacy Risks Planned Actions Log		
3.	Integrate PIA recommendations into system design	3.01	Project Requirements		Includes stakeholder and transition requirements specification.
		3.02	Solution Design and equivalent artifacts		Solution context documentation like architecture and related technical design docs.
		3.03	Privacy Risk Communication Plan		Carries communication plan that provides insights on how and when will privacy progress updates be shared with the wider group (includes assurance officer / team as well as Assurance Forum)
4.	PIA assurance (testing focused)	4.01	Privacy Test Plan & Privacy Exit Criteria		
		4.02	Privacy Test Inputs / Outputs		Includes test cases definition, test data, test / defect log, test summary etc.
		4.03	Privacy test sign-off document		
5.	Data Privacy Readiness Review	5.01	Test Completion Criteria		Completed Exit criteria document.
		5.02	Data Privacy Transition Plan		Includes knowledge transfer & training artifacts, updated to privacy risk register.
		5.03	Data Privacy Incident / Breach Reporting Process		
		5.04	Privacy Readiness Go Template		

Disclaimer

The documents and materials provided herein are for informational and conceptual purposes only and may contain redacted, modified, or incomplete information. No warranties, express or implied, are made regarding the accuracy, completeness, or fitness for a particular purpose. By accessing, downloading, or using these documents, you agree that such use is at your sole risk.

The website and/ or document owner and its affiliates expressly disclaim any and all liability, including for any direct, indirect, incidental, or consequential loss or damage arising out of or in connection with the use of these materials.

== End of document ===

Integrating Data Privacy Risk Impact Assessment within your project delivery lifecycle.

Author : Delon Xavier | Contact : +61 432 043 705
Email : delon.xavier@techsemantic.com | https://www.delonxavier.com