The following privacy / security solutions and services should be evaluated for all Major/Large IT enabled projects and projects collecting or storing significant volumes of High or Very-High risk information. This checklist is to be utilized when assessing the functional and technical requirements fit prior procurement. The guide is intended to outline core security services and integrations relevant to system implementations. The scope of the solutions implemented both informs the scope of the PIA, and provides assurance that the solution has been securely implemented. The PIA checklist should be reviewed when defining Functional and Technical Requirements, subject matter experts should be consulted, and cost estimates for each of the applicable services must be identified (where applicable) and integrated with project cost. Additionally, the completed PIA checklist should be provided to [pia.process@ubc.ca](mailto:pia.process@ubc.ca) identifying the solutions & services to be implemented.

| # | Security Integration/Service | What does the solution do? | PIA Checklist (Check all that apply) |
| --- | --- | --- | --- |
| 1 | Identify and Access Management (IAM) & Campus Wide Logon(CWL)  *Contact* [sebastian.gonzalez@ubc.ca](mailto:sebastian.gonzalez@ubc.ca) | The Campus Wide Login (CWL) suite of services to lower administration effort of managing accounts, improve user experience and reduce privacy and security risk by increasing compliance. Services include:   * authentication * authorization * automated provisioning and de-provisioning of accounts * provisioning of information to vendors (identifiers, tokens, attributes) * provision of privacy notification and collection of consent * Multi-factor authentication (MFA) and authorization | CWL used for authentication  CWL used for authorization  Automated provisioning/de-provisioning  CWL used for privacy notification/consent gathering  MFA authentication and authorization  Not applicable |
| 2 | Log Consolidation Service  *Contact:*  steve.rosco@ubc.ca | Log consolidation is a service to capture and monitor key security related logs from UBC systems. The service assists service owners to:   * Comply with ISS-17 * Identify security events impacting their system identification logic | Log consolidation used for application authentication logging only (CWL logs captured)  Mobile application authentication captured in logs  Application & System logs reviewed and integrated  Not applicable |
| 3 | Data Governance & Integration Services Offered by the Integration Enablement Center (IEC) via EDI  *Contact:*  [marcela.hernandez@ubc.ca](mailto:marcela.hernandez@ubc.ca) | The new system must ensure that it meets the data definitions as per the University Data Model and assists in proper management of UBC digital information.  The IEC enables development of secure, scalable interfaces between UBC service providers (internal and external) where the data being shared follows standard approved processes, approved by data owners and PIA requirements. | Data Governance team contacted and data definitions meet University Data Model  Integrations via EDI  Point-to-point integrations  Data custodian approved access and disclosure of PI attributes  Not applicable |
| 4 | Source Code Analysis  *Contact:*  [armenak.grigoryan@ubc.ca](mailto:armenak.grigoryan@ubc.ca)  aaron.heck@ubc.ca | Automatically reviews code of in-house developed systems or other systems where we have the source code for poor coding practices, many of which could result in unintended access to systems/information.  Assist in meeting compliance with ISS#20. | Source code review scheduled prior to go-live  Ongoing schedule for pre-production code review in-place with known support resources  Not applicable |
| 5 | Vulnerability and Web Application Scanning  *Contact:*  [security@ubc.ca](mailto:security@ubc.ca) | Vulnerabilities in infrastructure, middleware and applications are discovered all the time. Scans detect known vulnerabilities in software packages and detect weaknesses in applications caused by poor coding practices & system administration. | Vulnerability and application scanning scheduled or performed  Ongoing responsibility for receipt, interpretation and remediation of findings allocated  Not applicable |
| 6 | Cloud Vendor Scorecards  *Contact:*  pia.process@ubc.ca | Cloud vendor scorecard provides 'outside-in' report card of the security risk posture of an organization. The scorecard continuously gathers security intelligence data and instantly grades companies from A to F across ten crucial security categories. | Cloud vendor report reviewed prior to procurement  Cloud vendor continuous monitoring required  Not applicable |
| 7 | Payment Card Industry (PCI) Integration  *Contact:*  [raul.ramos@ubc.ca](mailto:raul.ramos@ubc.ca) | All UBC payment card merchants that store, process, or transmit Card Holder Data (CHD) as payments to UBC and / or operate Point of Sale (PoS) systems and devices must comply with PCI Data Security Standards (DSS). | PCI compliance required  PCI compliant  Not applicable |
| 8 | Data Discovery & Anonymization  *Contact:*  armenak.grigoryan@ubc.ca | UBC service to anonymize personal information with identifiers to mask such information and to ensure that personal information is not unnecessarily stored in non-production environments. | Consult on data anonymization service for feasibility  Not applicable |
| 9 | Web Application Firewall  *Contact:*  [aaron.heck@ubc.ca](mailto:aaron.heck@ubc.ca)  [security@ubc.ca](mailto:security@ubc.ca) | Application layer protection on potential security vulnerabilities must be considered prior to implementation. This service is currently only applicable to on premise solutions. | Web application firewall implemented  Not applicable |