

The Jonesi Consultancy | Houston, TX

EXECUTIVE AI ADOPTION · REVIEW WORKSHEET

INTEGRATION SECURITY REVIEW



Validate. Protect. Integrate with Confidence.

*Every unchecked item is either an open task or an accepted risk.
Record which one it is.*

1 Integration Security Review

Complete this review before any AI tool is connected to a live system or a real data set. Mark each item complete, open, or not applicable.

INTEGRATION NAME _____	SYSTEM / SERVICE _____	VENDOR / PROVIDER _____	INTEGRATION TYPE _____
BUSINESS OWNER _____	TECHNICAL OWNER _____	REVIEWER _____	DATE / ENVIRONMENT _____

AUTHENTICATION & IDENTITY

- ☐ Strong authentication is supported
- ☐ Multi factor authentication is available
- ☐ Service accounts are used rather than personal accounts
- ☐ Tokens and keys are scoped to least privilege
- ☐ Credential rotation policy is defined
- ☐ Revocation process is documented and tested

PERMISSIONS & ACCESS

- ☐ Access is granted on a least privilege basis
- ☐ Roles and permissions are well defined
- ☐ Data access scope is limited to what is required
- ☐ Administrative access is restricted and monitored
- ☐ Access reviews are scheduled and documented
- ☐ Permissions have been tested and validated

ENCRYPTION & DATA PROTECTION

- ☐ Data is encrypted in transit
- ☐ Data is encrypted at rest
- ☐ Current encryption standards are in use
- ☐ No sensitive data appears in URLs, logs, or headers
- ☐ Key management process is defined
- ☐ Backup data is encrypted and access controlled

PRIVACY & DATA MINIMIZATION

- ☐ Only necessary data is shared
- ☐ Personal and regulated data is identified
- ☐ Anonymization or masking is applied where possible
- ☐ Data retention period is defined
- ☐ Deletion and disposal process is defined
- ☐ Privacy impact assessment is complete

REGULATORY & COMPLIANCE

- ☐ Applicable regulations are identified
- ☐ Vendor provides compliance attestations
- ☐ Data residency requirements are met
- ☐ Cross border data transfer is reviewed
- ☐ Contracts and data processing terms are in place
- ☐ Audit rights and reporting are defined

CONNECTION SECURITY

- ☐ All endpoints use secure transport only
- ☐ Input validation is enforced
- ☐ Rate limiting or throttling is enabled
- ☐ Protection against injection attacks is in place
- ☐ API keys and tokens are stored securely
- ☐ Webhooks use verified signatures

VENDOR EVALUATION

- ☐ Vendor security practices have been reviewed
- ☐ Independent security certification is provided
- ☐ Vendor financial stability is assessed
- ☐ Incident response process is documented
- ☐ Uptime commitments meet business needs
- ☐ Subprocessors and third party usage disclosed

MONITORING & ALERTING

- ☐ Availability is monitored
- ☐ Real time alerts are configured
- ☐ Anomaly detection rules are in place
- ☐ Failed requests and errors are tracked
- ☐ Performance metrics are collected
- ☐ Alert escalation paths are defined

LOGGING & AUDIT TRAIL

- ☐ All integration activity is logged
- ☐ Logs capture user, action, and timestamp
- ☐ Logs are tamper resistant and protected
- ☐ Log retention period is defined
- ☐ Audit logs are accessible to reviewers
- ☐ Logs are reviewed on a set cadence

TESTING & VALIDATION

- ☐ Functional testing is complete
- ☐ Security testing is complete
- ☐ Data integrity testing is complete
- ☐ Error handling has been tested
- ☐ Failover and resilience have been tested
- ☐ Results are reviewed and approved

ROLLBACK & INCIDENT RESPONSE

- ☐ Rollback plan is documented
- ☐ Rollback process has been tested
- ☐ Incident response plan is defined
- ☐ Stakeholders and contacts are identified
- ☐ Communication plan is defined
- ☐ Data recovery plan is in place

MAINTENANCE & LIFECYCLE

- ☐ Integration owner is assigned
- ☐ Maintenance and update process is defined
- ☐ Change management process is defined
- ☐ Dependency tracking is in place
- ☐ Periodic review schedule is set
- ☐ Decommission plan exists

2 Risk Rating and Approval Complete Before Go Live

☐ LOW RISK

All critical controls are in place. Risk is acceptable. Proceed.

☐ MODERATE RISK

Some controls need improvement before go live. Document the plan.

☐ HIGH RISK

Significant gaps exist. Do not proceed until they are closed.

☐ CRITICAL RISK

Unacceptable risk. Escalate immediately.

BUSINESS OWNER APPROVAL

Name & date

TECHNICAL OWNER APPROVAL

Name & date

SECURITY REVIEWER APPROVAL

Name & date

NEXT REVIEW DATE

Name & date

CHECK THOROUGHLY. INTEGRATE SECURELY. REVIEW REGULARLY.

Re-run this review at every renewal, every major vendor release, and any time the scope of data access changes. Strong integrations, stronger outcomes.

© 2026 The Jonesi Consultancy. All rights reserved.

Validate. Protect. Integrate with Confidence.

We help organizations set the lines, train to them, and put governance behind them.

