

Black Duck® Software Risk Manager™ – Standalone Implementation Package

The services described in this Software Risk Manager Implementation Package (the "**Services**") are provided by Black Duck® and/or its Affiliates (collectively, "**BD**") to Customer in accordance with the terms of this Software Risk Manager Implementation Package (this "**Services Package**") and are subject to the terms and conditions of the Purchasing Agreement and the End User License and Maintenance Agreement pursuant to which these Services have been purchased by Customer, or where no such agreement governing the Services to be provided is referenced therein, the most recent version of the End User License Agreement posted at <https://www.blackduck.com/company/legal/end-user-licenses.html> (collectively, the "**Agreement**"), and such terms and conditions are incorporated herein by reference. All capitalized terms that are not defined in this Software Risk Manager Implementation Package will have the meaning set forth in the Agreement.

1 Overview

Black Duck's Software Risk Manager Implementation Packages help customers get acquainted with Software Risk Manager. These packages provide a structured and guided approach to help implement and adopt Software Risk Manager.

BD offers the Software Risk Manager Implementation Packages in QuickStart Plus and Pro tiers and includes:

Description	QuickStart Plus	Pro
Software Risk Manager Server Installation	✓	✓
Account creation and Identity Access Management (IAM) integration	✓	✓
Supported Tool Connectors Enabled	Up to 2 tools	Up to 5 tools
Codebase(s) onboarded	1	Up to 2
Automation through CI/CD integration (Jenkins, Team City, Bamboo)	✓	✓
Workflow through issue tracker integration (Jira, ADO, ServiceNow, Gitlab) with one supported application		✓
Third-party integration (Burp Suite, OWASP ZAP, Splunk)		1
Results review	1	Up to 2
Training	CBT Only	✓

1.1 Package Delivery Success Criteria

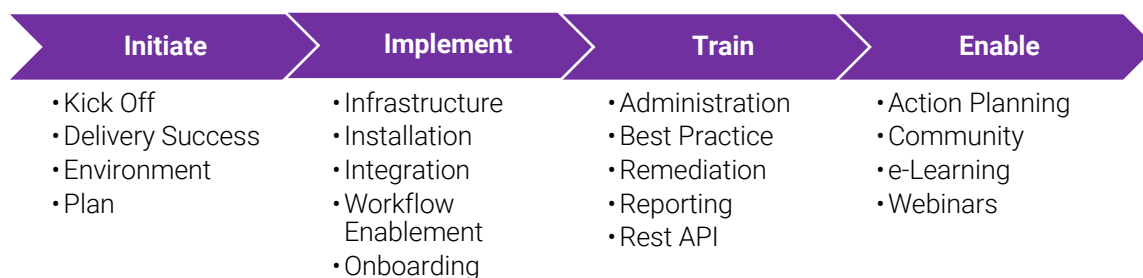
The following table outlines the criteria BD measures for successfully completing the Services.

Item	Criteria
1	Software Risk Manager instance is "Production Ready": - Coverity has been installed and tested in the Customer's environment. - End-user access provisioned and successfully tested - Maintenance and upgrading procedures have been reviewed and discussed.
2	Designated Codebase(s) and respective project team(s) have been onboarded per Section 2.2 below.
3	Software Risk Manager best practice guidance provided to the in-scope Codebase(s) project team(s) and designated product champion(s).
4	In-scope product features have been enabled and demonstrated to the relevant project team(s).
5	Customer administrator(s) have been identified and trained in Software Risk Manager administrative functions.
6	The integrations designated in Section 2.2 are enabled, tested, and members of the in-scope project team(s) are trained on their usage.
7	Developer workflows reviewed, enabled, and tested for alignment with BD best practices and fulfillment of Customer's usage requirements.
8	Customer has been guided on post-implementation support, including self-paced online training, Community Portal, and technical support access.
9	An Action Plan to identify the completed tasks and recommend next steps have been reviewed and discussed with the Customer.

2 Implementation Approach

BD will assist Customer with deploying Software Risk Manager, onboarding the in-scope Codebase(s), and facilitating developer adoption. The overall process consists of four phases, as described below.

Figure 1: Phases



2.1 Initiate

BD and Customer will conduct the Initiate Phase in one or more meetings with the following objectives.

- **Kick-Off** – Review Customer’s goals and organizational outcomes. Identification of Customer stakeholders for the following functions:
 - Project management,
 - Infrastructure – network, hardware, database, and security,
 - Project team leader(s) – the owner of teams pioneering adoption,
 - Integrated application engineers – owners of tools/systems with which Software Risk Manager will integrate; and
 - Customer evangelists – members of the Customer’s teams identified as the critical leaders for adoption and success.
- **Requirements** – Customer confirmation of elements to be completed for the delivery.
- **Success Criteria** – Confirm the success criteria as they relate to the scope:
 - Production-ready – Software Risk Manager is operational,
 - Third-party integrations – continuous integration,
 - Development team – trained in scanning best practices, tool usage, and remediation, and
 - Administrators – trained in configuration, tool usage, and reporting.
- **Delivery Process** – Review the Software Risk Manager implementation process:
 - Target goals: short-term, near-term, long-term,
 - A sample project plan for the first 90 days, and
 - Establish Customer champion and implementation point of contact.
 - Environment – Establish the initial environmental needs.
 - Software Risk Manager deployment method.
- **Plan** – Identify a plan of action to designed ensure Services are completed in a timely manner.

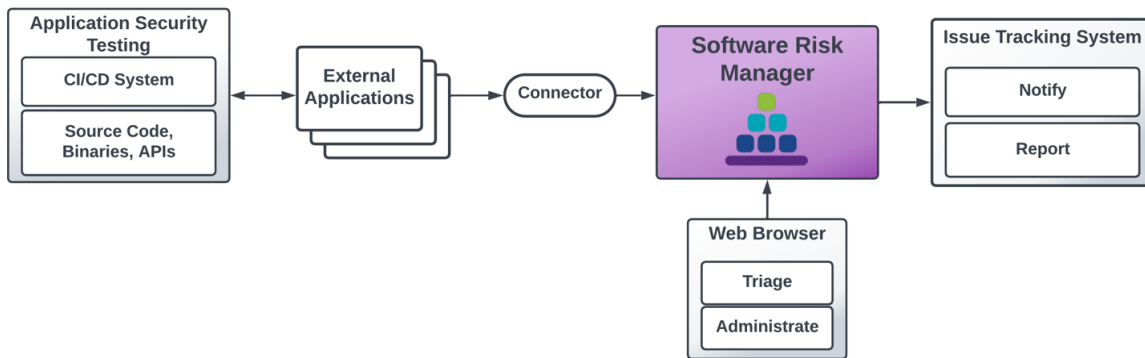
2.2 Implement

2.2.1 Infrastructure Deployment

BD will assist with the installation and configuration of Software Risk Manager as per Customer's selected implementation package:

Description	QuickStart Plus	Pro
Installation of one (1) Software Risk Manager server instance	✓	✓
User authentication integration with LDAP/SAML	✓	✓
Setup of users, groups, roles, and responsibilities	✓	✓

Figure 2: Deployment Architecture



Software Risk Manager supports several different methods for installation, such as Docker, Kubernetes, Linux, and Windows. The Software Risk Manager installer is self-contained, it includes all the software necessary to run Software Risk Manager and depends on its own Tomcat, Apache, and MariaDB services. Software Risk Manager is a web-based application. Using your browser, you can navigate the user interface (UI) to perform product administration, project management, and triage.

Tool connectors allow Software Risk Manager to pull results directly from external tools and applications without manually exporting the results from those tools and uploading them into Software Risk Manager.

Issue Tracker, if configured, enables the workflow engine to push issues through Software Risk Manager to an external issue tracking system, such as Jira, ADO, ServiceNow, or Gitlab.

Scanners, both built-in dependency and code scanners, will analyze the source using bundled tools built specifically for a target language.

BD assists customers with the setup and configuration of Software Risk Manager. Once complete, BD will review the connectivity to their Software Risk Manager server.

BD will assist with third-party integrations of the following systems:

- One (1) third-party user authentication integration (via LDAP or SAML); and
- Assistance with the setup of users, groups, roles, and responsibilities.

2.2.2 Onboarding

BD will assist with the onboarding of the in-scope Codebase(s) onto Software Risk Manager.

Description	QuickStart Plus	Pro
Codebase Onboarding	1	Up to 2
Supported Tool Connectors Integrations Enabled	Up to 2	Up to 5
Results Review Session	1	Up to 2

Codebase Onboarding - BD will aid the Customer through the onboarding, installation, and configuration of a project and results review.

During the onboarding of each in-scope Codebase BD will:

- Complete an initial scan of the Codebase and conduct a scan review session with Customer representatives.
- Review initial scan results and triage best practices.

Codebase means source code with the following attributes:

- Checked out from the same source code management (SCM) repository
- Uses the same compiler for a given supported programming language
- Utilizes the same build infrastructure and scripts
- If multiple checkouts are required (each building a particular component or microservice), then each checkout:
 - Comprises a part of a cohesive system, and
 - Consistently communicates with other components (e.g., direct function call, library, or REST API) to provide the required functionality.

Tool Connectors Integration - BD will aid the Customer through the supported tool connectors integration(s).

Results Review - BD works with Customer's representative security team member to assess the first set of vulnerabilities. BD will aid Customer with identifying high-risk issues and prioritizing vulnerabilities for remediation.

Through this process, BD will:

- Educate Customer on the high/must-fix vulnerabilities found on the in-scope applications.
- Recommend a process for categorizing and prioritizing defects found based on risk.
- Select high severity vulnerabilities for review with Customer stakeholders.

2.2.3 Workflow Integration

BD will aid with integrating Software Risk Manager with Customer's tools and development processes through Software Risk Manager's supported integrations. BD will complete the tasks listed in the table below for each in-scope application.

Description	QuickStart Plus	Pro
CI/CD Integration	1	Up to 2
Issue Tracker Integration (Jira, ADO, ServiceNow, Gitlab)		1
Integration with third-party applications (Burp Suite, OWASP ZAP, Splunk) via supported Plug-ins		1
IDE Integration (Eclipse, Visual Studio, IntelliJ)		✓

BD will aid the customer with the following third-party integrations:

- In the QuickStart package with one (1) third-party CI/CD integration.
- In the Pro package with:
 - Two (2) third-party CI/CD integrations, such as Jenkins, Bamboo, or Team City.
 - One (1) third-party Issue Tracker Integration (ITS), such as Jira, ADO, ServiceNow, or Gitlab.
 - One (1) third-party application, such as Burp Suite, OWASP ZAP, or Splunk via supported plug-ins.

CI/CD Integration – Software Risk Manager fits into the CI/CD pipeline (Jenkins, Bamboo, Team City, etc.); it enables organizations to implement DevSecOps by automating application security processes throughout the entire SDLC, consolidating all AppSec activities into one place.

Issue Tracker Integration – Software Risk Manager provides a two-way issue tracker integration (Jira, ADO, ServiceNow, Gitlab, etc.) to assign findings to projects and users.

IDE Integration – Software Risk Manager IDE plug-ins (Eclipse, Visual Studio, IntelliJ) streamline the use of Software Risk Manager within the integrated IDE to assist developers push new builds for Software Risk Manager analyses and review the results from within the IDE.

The Software Risk Manager workflow provides a 360-degree view to users of the risk for each integrated application: custom code, third-party component(s), and network where the software resides.

BD will aid with third-party IDE Integrations, such as Eclipse, Visual Studio, and IntelliJ via supported plug-ins.

Included in the Pro package, for each in-scope Codebase, BD will assist in deploying the IDE plugin to one (1) developer workstation. Developers will have the ability to view the centralized results for their project directly in their IDE.

2.3 Train

Description	QuickStart Plus	Pro
Self-paced online training	✓	✓
One (1) end-user training (up to 16 end users)		✓

Training – Training topics include:

- **Administration** – Configuration of users, groups, projects, and project fields.
- **Basic Tool Usage & Best Practices** – Review of tool functionality, risk visibility, and results review.
- **Reporting** – Review of Software Risk Manager reports and REST APIs.

Documentation – BD will make available to Customer a report that will help guide Customer's use and maintenance of Software Risk Manager, which will include:

- A report on how the Software Risk Manager is deployed and
- A review of the implementation steps carried out during the engagement.

2.4 Enable

The Enable Phase ensures Customer is set up for success and is ready to begin using Software Risk Manager. At the start of this phase, BD will complete an Action Plan outlining the recommended activities for Customer's continued adoption of Software Risk Manager. The Action Plan provides Customer with:

- A summary of the steps completed during the execution of the service package.
- An assessment of Customer's maturity as it relates to BD's product maturity model.
- Recommended next steps to mature Customer's implementation,
- Instructions to access:
 - The Community,
 - Online product training and
 - Webinars.

BD will review the Action Plan with Customer for final sign-off and transition Customer to the BD Customer Success team.

3 Scope of Services

Licensed Product covered by this Services Package:

Product	Version
Software Risk Manager	Currently Supported Versions

4 Prerequisites and Dependencies

Entry Criteria - The following is a list of requirements and dependencies that the Customer must meet to enable BD to perform the Services:

1. Provide a primary point of contact with a deep understanding of the requirements.
2. Verify receipt of a valid license file for Software Risk Manager.
3. Verify that hardware meeting the minimum requirements (described in the Software Risk Manager Installation Guide) has been secured.
4. Identify the Project Team(s) the BD consultant will work with for the Services delivery.
5. Provide access to infrastructure, security, database, and network teams to assist with any hardware or networking issues.
6. Remote access for hands-on activities by BD staff is available.
7. If onsite, provide office space for the BD consultant.

If Customer fails to meet the prerequisites and dependencies described above, and to the extent that BD cannot perform the Services because of Customer's failure to meet those prerequisites and dependencies, BD will not be obligated to perform the affected Services.

5 Location of Performance of Services

Services will be delivered remotely.

Onsite delivery is available at an additional cost and requires a signed agreement. Travel and expenses for the onsite delivery will be billed separately based on actual costs.

6 Purchasing Agreement

The parties shall mutually agree to the schedule for the performance of the Services, subject to the terms of the Agreement and this Service Package. All Services described within this Services Package must be used within one year of the Start Date set forth in the Purchasing Agreement pursuant to which this Services were purchased. Unused services are non-refundable and non-transferable pursuant to the terms and conditions of the Purchasing Agreement. Performance of Services is subject to scheduling and Customer availability.

End of Services Package