

Black Duck® Software Risk Manager™ – Integrated 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

BD's Implementation Packages aid customers who are getting acquainted with Software Risk Manager. These packages provide a structured and guided approach to help with Software Risk Manager's implementation and adoption.

The Software Risk Manager Implementation Packages are offered by BD in Pro and Premier tiers, and include:

Description	Pro	Premier
Software Risk Manager Server Deployment	✓	✓
Codebase Onboarding	✓	✓
Workflow Integration	✓	✓
Advanced Workflow – Break-the-build	✓	✓
Advanced Workflow – Pull Request Annotations		✓
Issue Tracker Integration (Jira, ADO, ServiceNow, Gitlab)	✓	✓
Instructor-led Training	✓	✓
Onboarding Runbook		✓

1.1 Package Delivery Success Criteria

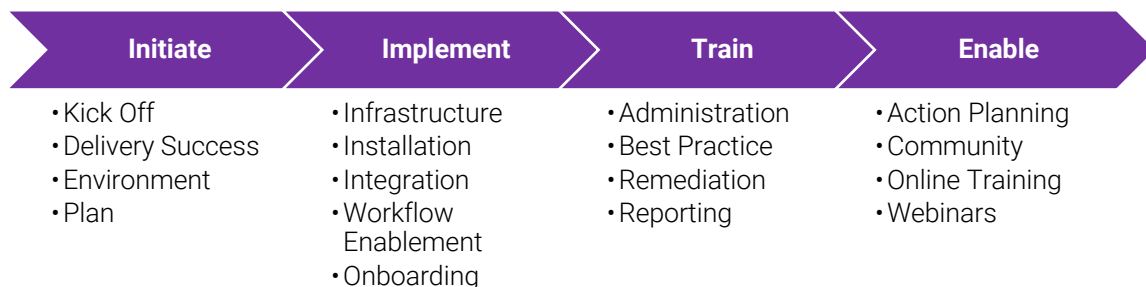
Item	Criteria
1	Software Risk Manager instance is "Production Ready." • Software Risk Manager has been installed and tested in the Customer's environment. • End-user access provisioned and successfully tested. • Maintenance and upgrading procedures have been reviewed and discussed.
2	Designated Codebase(s) and respective project team(s) have been onboarded per Section 2.2.

Item	Criteria
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 in-scope integrations designated in Section 2.2 are enabled and tested; 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 recommended next steps have been reviewed and discussed with the Customer.

2 Implementation Approach

BD will assist Customer with onboarding groups of developers onto Software Risk Manager and will facilitate developer adoption. The overall process consists of four phases, as described below.

Figure 1: Phases



2.1 Initiate

The Initiate Phase will be conducted by BD and Customer 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, database, and security;
 - Project team leader(s) – owner of teams pioneering adoption;
 - Integrated application managers – owners of tools/systems with which Software Risk Manager will integrate; and/or

Version 2024.11

Implementation – Software Risk Manager - Integrated; Product Numbers: 57183-0, 57184-0

- Customer evangelists – members of the Customer's teams identified as the critical leaders for adoption and success.
- **Requirements** – Customer confirmation of what elements of the Services are applicable.
- **Success Criteria** - Confirm the success criteria, as they relate to the scope:
 - Production-ready – Software Risk Manager is operational;
 - 3rd party integrations – continuous integration/deployment, notifications, bug tracking systems;
 - 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 Server and Analysis deployment method.
- **Plan** – Identify a plan of action designed to 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 per Customer's selected Implementation package:

Description	Pro	Premier
Software Risk Manager Server Installed	✓	✓
User Authentication Integration (LDAP/SAML)	✓	✓
Role-based Access Control (RBAC) Configuration	✓	✓
Backup Procedures Automated	✓	✓
Configure SMTP and Notifications	✓	✓

Software Risk Manager Server Deployment – Software Risk Manager is a web-based application. Using a browser, Customer can navigate the user interface (UI) to perform product administration, project management, and triage.

BD will assist Customer with installing and configuring Software Risk Manager on one(1) host server. Once complete, BD will review the connectivity to their Software Risk Manager server.

Third-party integrations of the following systems will be configured:

- One (1) third-party user authentication integration (via LDAP or SAML); and
- One (1) email (SMTP) server.



Users, groups, roles, and responsibilities in the Software Risk Manager UI will be set up to comply with Customer's RBAC rules.

Automatic backups of the Software Risk Manager database will be configured.

2.2.2 Codebase Onboarding

BD will assist with the onboarding of the in-scope codebase(s) into Software Risk Manager to meet the usage plans described in this Services Package:

Description	Pro	Premier
Codebases Onboarded	One (1)	Two (2)
Project(s) and Subproject(s) Created	✓	✓
Enable SCM Integration	One (1)	Two (2)
Install Black Duck Bridge and Configure SAST and SCA Settings	✓	✓
Results Review	✓	✓

Codebase is 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.

Project Baseline / Scan Tuning and Configuration – During the onboarding of each in-scope Codebase, BD will:

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

Projects are used to organize codebases and applications in Software Risk Manager. There may be a single project for a codebase or a project with sub-projects representing an application.

BD will aid Customer with creating and configuring Project(s) and Subproject(s), setting up the hierarchy in accordance with best practices to align with the Customer's organizational and application structure.

Black Duck Bridge – The BD Bridge Command Line Interface (Black Duck Bridge) allows you to run scans and receive results from the command line by scripting or running the commands manually. Black Duck Bridge invokes adapters that handle SAST and SCA scanning and abstracts the various extensions and variables for them.

AST Settings – Software Risk Manager can be licensed to include SAST and SCA scanning capabilities; any mention of these terms in this document refers to those built-in licensed capabilities, not any other SAST/SCA tool.

Version 2024.11

Implementation – Software Risk Manager - Integrated; Product Numbers: 57183-0, 57184-0

BD will aid the Customer in configuring appropriate AST scan settings for the in-scope Codebase(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 in the in-scope Codebase(s).
- Recommend a process for categorizing and prioritizing findings found based on risk.
- Select high-severity vulnerabilities for review with Customer stakeholders.

2.2.3 Workflow Integration

BD assists with integrating Software Risk Manager with Customer's tools and development processes. The following tasks will be completed for each in-scope Codebase:

Description	Pro	Premier
Policy setup and configuration	✓	✓
Email notification configuration	✓	✓
CI/CD Integration	✓	✓
Additional Ingress Tool Connector Integration	1	2
Issue Tracker Integration (Jira, ADO, ServiceNow, Gitlab)	✓	✓
Code Sight (IDE plugin) configuration	✓	✓
Break-the-build Workflow	✓	✓
Pull Request Annotations		✓

Policies in Software Risk Manager allow you to track compliance to specified requirements. Once defined, policies can be applied to projects, and policy violations can be monitored. In this way, policies can be used to prioritize which security issues need to be addressed, how often scans should be scheduled, and so on.

Email notifications can be set up to notify of policy violations.

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

Supported ingress tool connectors can be configured to pull in data from other AppSec tools for your projects.

Issue Tracker - Software Risk Manager provides a two-way issue tracker integration (Jira, ADO, ServiceNow, Gitlab, etc.) to assign findings to projects and users. One (1) issue tracker system will be integrated with Software Risk Manager for each in-scope Codebase.

Code Sight is a plugin that can be installed and configured on supported IDEs. The plugin allows users to view Software Risk Manager findings directly in their IDE.

Break the Build - Policies can be leveraged to break builds executed by the Black Duck Bridge.

Pull Request Annotations - Software Risk Manager fits into the Pull Request workflow. Automated scans can be set up on Pull Request builds to look for new findings before they are merged. Premier package

Customers will be provided a script to integrate with their CI/CD tool, so that these new findings can be annotated on the Pull Request (e.g. comments).

2.3 Train

Description	Pro	Premier
Self-paced online training	✓	✓
One (1) end-user training session (Up to 16 participants)	✓	✓

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 Software Risk Manager is deployed.
- A review of the implementation steps carried out during the onboarding.

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.

2.4 Enable

Description	Pro	Premier
Action Plan	✓	✓
Runbook		✓

This phase ensures Customer is set up for success and is ready to begin using Software Risk Manager.

Action Plan - 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 product maturity model;
- Recommended next steps to mature Customer's implementation; and
- Instructions to access:
 - The Community,
 - Online product training, and
 - Webinars.

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

Runbook - For Premier package Customers, BD will create a Runbook that will help guide Customer to self-onboard additional codebases. The Runbook will provide Customer with step-by-step instructions on:

- Setting up the project in Software Risk Manager

Version 2024.11

Implementation – Software Risk Manager - Integrated; Product Numbers: 57183-0, 57184-0



- Running analysis capabilities (SAST, SCA)
- Integrating with CI/CD automation
- Enabling policies
- IDE Integration

The Runbook will be customized for Customer's project language(s), CI/CD infrastructure, and SDLC workflow.

3 Scope of Services

The scope of Services is limited as follows:

Package	Codebases
Pro	One (1) Codebase
Premier	Two (2) Codebases

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. Download installer of Software Risk Manager.
3. Review the Documentation and secure hardware that meets the minimum requirements for:
 - One (1) Software Risk Manager server, and
 - One (1) build server for in-scope Codebase(s).
4. Verify receipt of a valid license key for Software Risk Manager.
5. Identify the Codebase(s) that Software Risk Manager will analyze.
6. Ensure a successful regular build (i.e., not using Licensed Product) of each Codebase has been completed on the build server (if applicable, i.e., the Codebase uses a compiled language).
7. Provide access to system administration assistance for any hardware or networking issues.
8. Provide office space for the BD while onsite (if applicable).
9. Provide access to:
 - The build server(s);
 - The Software Risk Manager server; and
 - Access could be through remote desktop or virtual network computing ("VNC"), screen sharing, or direct physical access to those hosts.

Version 2024.11

Implementation – Software Risk Manager - Integrated; Product Numbers: 57183-0, 57184-0

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