# RISK MANAGEMENT POLICY

| | |
|---|---|
| Version Number: | 1.0 |
| Version Date: | 10/09/2025 |
| Owned by: | Security, GRC |
| Approved by: | Nate Fitch, Sr. V.P., Chief of Staff |
| Confidentiality Level: | Internal |

# Table of Contents

# 1. Purpose

The Security team's mission is to reduce the likelihood and impact of security incidents in the Docker ecosystem. The security risk management program should enable a security-conscious culture empowering employees to surface relevant risks to help inform product and business decisions.

Docker has designed and implemented an agile risk-based approach to identify, evaluate, treat, and monitor risks until they have been reduced to the extent that is acceptable to Docker.

The security risk management program will be commensurate with Docker's size, complexity, and operational structure. In its current state, Docker as a growth phase technology company, requires an agile and flexible framework which is designed to enable an efficient and effective way of surfacing risks from various internal or external sources–including, but not limited to, audits, vulnerability scans, security incidents, penetration tests, code reviews, security reviews, gap assessments, regulatory changes, vendor activities, and emerging technologies.

In order to achieve this, Docker employees with a role to play in Security Risk Management should use their judgement on when a risk needs to be tracked vs. simply treating the risk to avoid unnecessary overhead.

This policy reinforces a culture of accountability and continuous improvement, supporting Docker's ISMS and commitment to trusted, secure operations.

# 2. Scope

This policy applies to all Docker business units, personnel, vendors, and processes within the operational and information security scope of Docker's ISMS. It covers technology, infrastructure, people, third parties, products, and business operations where risk must be proactively identified and managed.

# 3. Roles and Responsibilities

| **Roles** | **Responsibilities** |
|---|---|
| Executive Leadership | Executive sponsor authorizing this policy and its enforcement. Establishes a culture of risk awareness and ensures sufficient resources, authority, and oversight are in place to support security risk management. |
| Head of Security, Risk & Trust | Owns the risk management framework and risk register, facilitates annual reviews, drives remediation planning, and ensures alignment of risk mitigation strategies with corporate objectives. Also responsible for enforcing policy compliance and continuous program improvement. |

| | |
|---|---|
| Domain Leads | Domain Leads that are responsible for setting goals and priorities for their respective Domain. They act as escalation points when material misalignments arise and trade-offs are needed between security risk mitigation and the goals and priorities established for their teams. |
| Risk Owner | Members of Domain teams and centralized functions, are responsible for prioritizing and treating security risks they own based on goals and priorities established for their respective domains by their Leads. A Risk Owner can be a Domain Lead. |
| Risk Champions | SME's responsible for identifying, evaluating, and recommending solutions for risks in their respective domains using a consistent framework, during their respective workflows (vulnerability scans, code reviews, security reviews, penetration tests, gap assessments, security audits, etc) |
| GRC SME | Members of the GRC team who are responsible for maintaining the security risk management process, and ensuring security risks are consistently identified, evaluated, treated, and monitored through the security risk management lifecycle. |
| All Employees and Contractors | Expected to identify and report new risks, anomalies, or control deficiencies through established channels. Must support implementation of mitigation plans where applicable and participate in awareness programs that reinforce risk-informed behavior. |

# 4. Definitions

**Information Security Management System (ISMS)** - A systematic approach to managing sensitive company information encompassing people, processes, and technology to ensure information security through risk management, policies, procedures, and controls aligned with ISO 27001 standards.

**Risk Owner** - The individual accountable for prioritizing and treating a specific security risk based on their domain's goals and priorities, with authority to decide on risk treatment options (avoid, mitigate, accept, or transfer).

**Risk Champion** - A subject matter expert responsible for consistently identifying and evaluating security risks within their domain using the established risk assessment framework, and recommending treatment solutions during security workflows.

**Material Risk** - A security risk that could have significant impact on Docker's business operations, reputation, compliance status, or strategic objectives if realized, requiring escalation to leadership for prioritization decisions.

**Risk Register** - The centralized repository maintained by the GRC Team that records all identified security risks, including their description, assessment scores, ownership, treatment plans, and current status for tracking and monitoring purposes.

# 5. Security Risk Management Lifecycle

The end-to-end security risk management lifecycle has the following four stages:

1. **Identify** - This is the first stage of the security risk management lifecycle. Security risks can be identified by anybody at the company, but most of the security risk identification will be the result of workflows owned by the Security team.
2. **Evaluate** - This is the stage where identified security risks are evaluated using a consistent framework by Risk Champions.
3. **Treat** - This is a Risk Owner's response to an identified security risk. An identified risk can be treated by mitigation, acceptance, avoidance or transfer.
4. **Monitor** - Identified risks, their severity, and treatment will be monitored by Security Risk Analysts to ensure accountability, informed decision-making, and robust security governance.

## 5.1 Risk Identification

Docker employees are empowered and encouraged to surface security risks as part of their day-to-day activities. To support this, adequate channels have been established to enable employees to surface security risks. Additionally, the following formal programs shall be established to identify material security risks to Docker's business:

***Internal Security Reviews***
A formal internal security review process shall be established to enable the timely identification of security risks that may be introduced to new product development, new vendors, or material changes to our architecture.

***Security Risk Assessments***
Security risk assessments shall be conducted at least annually. Additionally, scenario-based risk assessments shall be performed on demand to gain a deeper understanding of key security risks significant to Docker.

***External Security Reviews***
Docker will rely on independent auditors and security researchers to stress test the design and operational effectiveness of our security controls stack through penetration testing, bug-bounty programs, and holistic audits of Docker's information security program (SOC 2, ISO27001). All of these independent efforts may aid in identifying security risks.

***Incident Response***
For events that require immediate risk mitigation and or response, an incident response program is maintained to ensure timely mitigation and response to applicable security events.

### 5.2 Risk Assessment Methodology

A framework shall be used to determine the likelihood and impact of security risks to Docker. This framework provides structured analysis and facilitates a consistent risk assessment process aligned with Docker's business.

### 5.3 Risk Treatment

A Risk Owner shall be assigned to adequately prioritize the treatment of the security risks they own. The Risk Owner shall be supported by the Security Risk Analyst and/or Risk Champion where needed to adequately prioritize and treat the risk.

Below are treatment options that can be exercised by the Risk Owner based on goals and priorities established for their respective domains by their Leads:

- **Avoidance:** Risk Owner avoids the identified risk by passing on the opportunity that created the risk in the first place.
- **Mitigation:** Risk Owner mitigates the risk by implementing new controls/safeguards and/or makes changes to any existing controls in order to lower the impact or likelihood of the risk, ultimately bringing the identified risk to an acceptable level. This may involve adding or enhancing prevention/detection/corrective measures.
- **Acceptance**: Risk Owner accepts the identified risk and any corresponding fallout. Docker requires a formal risk acceptance workflow which includes a written rationale for acceptance and depending on the criticality of the risk, signed approval from the responsible executive. Accepted risks are subject to periodic review to ensure their status has not materially changed, and they are re-evaluated as part of the annual ISMS review cycle.
- **Transfer**: Risk Owners transfer the identified risk to a third party, such as through insurance or contractual agreements with vendors or service providers. This does not eliminate the risk but reallocates its impact or responsibility. All risk transfers must be documented with clear roles and responsibilities. Risk Owners remain accountable for oversight and must review transferred risks periodically and during Docker's annual ISMS review cycle.

### 5.4 Risk Monitoring

Progress on risk mitigation shall be periodically monitored for adequacy. Adequate self-serve mechanisms for Risk Owners to be aware of the risks they own shall be established.

Material security risks that are not prioritized for treatment shall be communicated to security leadership and/or relevant Domain leads for adequate re-prioritization and determining the next course of action.

Key thematic security risks material to Docker's business shall be periodically (at least annually) presented to security and executive leadership.

## 6. Risk Register and Documentation

All risks will be recorded, triaged, and tracked via Docker's risk register, which is maintained by the GRC Team and accessible through established channels. The risk register will capture the following::

- The Description of the Risk
- When the Risk was identified
- The Risk Score and its corresponding analysis
- The Risk Owner and Risk Champion
- The Status of the risk
- Risk Treatment Plan (if applicable)

# 7. Enforcement and Exceptions

All Docker personnel are expected to comply with this policy in full. Failure to adhere may result in disciplinary action, up to and including termination of employment or contract. In cases involving willful misconduct, malicious activity, or violations of law, Docker may initiate legal proceedings. The organization reserves the right to monitor, audit, and inspect user activity on its systems to ensure compliance.

Any exceptions to this policy must be formally requested, documented, and approved by Docker's GRC or Legal team. Exception requests must clearly outline the business justification and associated risks, and should be submitted to Docker's Risk Submission Portal.

# 8. Change History

| Date | Version | Responsible Party | Description of Change |
|---|---|---|---|
| 10/09/2025 | 1.0 | Nate Fitch, Sr. V.P., Chief of Staff | Risk Management Policy Approval |
| 07/03/2025 | 0.9 | Chad Fryer, Sr. Security Engineer, GRC<br>Emre Ugurlu, Sr. Security Engineer, GRC | Risk Management Policy Creation |