Naverisk

Security and Operations Manual

June 2021

CONFIDENTIAL AND PROPRIETARY

Contents

1.0 Introduction

Naverisk™ provides enterprise-grade IT management software to businesses and government organizations worldwide.
This document describes the approach to quality management and security undertaken by Naverisk.

Internal controls and process excellence are core philosophies behind our success as a trusted vendor of mission critical core business systems.

The document is designed for customers, partners and relevant third parties to provide a system and security overview, company information and details of Security and Operations controls.

2.0 System overview

Naverisk provides secure, onsite and cloud based, enterprise IT management software. Naverisk is hosted and operated from multiple data centres. These data centres are audited annually in accordance with the AICPA's Service Organization Control (SOC) framework and are certified compliant with ISO 27001.
We also run weekly, monthly and quarterly security audits across our software stack.

The Naverisk platform has been designed based on the following core principles:

1. **Scalability.** Able to handle large and variable workloads via Amazon Web Services (AWS) cloud systems. Accordingly, the platform has been architected to be fully scalable, reliable and available.
2. **Security**. Software and network architecture has been built to meet the requirements of the most security-sensitive businesses, including complete control over where enterprise data is stored.
3. **Analytics.** Naverisk provides powerful reporting and analytics to collect and report on all system events.

The Naverisk cloud platform is implemented by a set of applications composed of proprietary code along with trusted third-party services. All interactions between users, administrators and modules are completed using standard cryptographic protocols, being Secure Socket Layer (SSL) or Transport Layer Security (TLS). As mandatory all Naverisk services use MFA.

3.0 People

Naverisk employs approximately 50 employees organized in the following functional areas:

- **Senior Leadership Team.** Consisting of the Chief Executive Officer (CEO) and senior staff responsible for running various functional units. In particular:
    - Chief Executive Officer
    - Chief Technology Officer
    - Chief Information Security Officer
    - Product Owner

- **Customer Success.** Provides technical support, training and business process guidance to customers.
- **Marketing.** Staff responsible for marketing and product improvement roadmaps.
- **Business Development.** Staff responsible for forging beneficial relationships in the market.
- **Engineering.** Staff responsible for developing and operating the Naverisk platform, while making improvements and enhancements required by the business.
- **Accounting, Finance and Human Resources.** Staff responsible for managing the financial and internal operations of the company.

4.0 Procedures

Our services are supported by the Naverisk Engineering & Customer Success teams 24 hours a day, 7 days a week, 365 days a year. The key support services include:

- System development and maintenance.
- Help desk for system users.
- Infrastructure support.
- Data centre operations and performance monitoring.
- Security administration and auditing.
- Implementation support and best practices guidance.
- Business recovery planning.

Logical Access. Access to the production network is restricted by an explicit least privilege basis. It is frequently audited, and is closely controlled by our Engineering team. Staff accessing the network are required to use multiple factors of authentication.

Penetration Testing and Vulnerability Assessments. Third party security testing of our service provider is performed by independent and reputable security consulting firms. Findings from each assessment are reviewed with the assessors, risk ranked, and assigned to the responsible team.

5.0 Software

Naverisk is developed and maintained by an in-house Software Engineering group. Their main focus is to enhance and maintain the Naverisk platform to provide best-of-breed experience to our customers and partners.

Our QA team reviews and tests our code base. Dedicated application engineers on staff identify, test, and triage security vulnerabilities in code. Secure source code version control and deployment methodologies, ensure source code and production environments are protected from catastrophe and casual degradation by human error or unintended consequences.

Separate Environments. Testing and staging environments are separated from the production environment. No actual customer data is used in the development or test environments.

6.0 Infrastructure

Naverisk is hosted and operated from multiple data Centre's operated by AWS. These data Centre's are audited annually in accordance with the AICPA's Service Organization Control (SOC) framework and are certified compliant with ISO 27001.

Regular data backups are performed for all information and stored on an external site. In a catastrophic situation where multiple data Centre's suffer a disaster; service would be restored within a few hours using backups. Service clustering and network redundancies eliminate a single point of failure.
All interactions between users, administrators and modules are done using the Secure Socket Layer (SSL) or Transport Layer Security (TLS) standard cryptographic protocols.

All services use MFA authentication for access. All external and internal correspondence such as email pass through security filters.

All devices have AV and security applications and policies activated.

7.0 Data

Data as defined by Naverisk consists of the following:

- Company and customer data residing in the database used to store customer data, configuration settings, usage logs, and other customer-specific system files and master code repositories.
- Error logs.

Access to data within Naverisk is governed by access rights, and can be configured to define access privileges.

8.0 Data Sovereignty

Naverisk's cloud service is hosted and operated from multiple data centre's operated by AWS, depending on the regional instance selected by the customer providing data sovereignty.

9.0 Security Management

Naverisk has implemented a number of security management controls:

- Established SOC security policies to address the classification and protection of information, the encryption and security of company data on laptops and mobile devices, encryption for data at rest and in transit as well as the acceptable use of information and systems.
- The Senior Leadership team has established roles within the organization to administer the company's security policies.
- To assist with the administration of the information security function, the Senior Leadership team has regular meetings and to make sure security controls and procedures for a specific system or group of systems are actioned and in place.
- All employees are required to sign and acknowledge their review of security policies.

The effective management of risk is of critical important to Naverisk. The Risk Management Policy sets out the goals and procedures by which the organisation will identify, control and mitigate risks to itself, and to its customers.

All employees and contractors are required to be aware of potential risks, and communicate any identified risks to Management in a timely manner so they can be assessed and appropriate action taken.

10.0 Risk Identification

Potential risks may be identified through the compliance of documented policies and by individuals adopting a "risk-aware" stance in their day-to-day job activities. This means risks are identified both proactively and reactively. Risks are generally identified from:

1. Regular monthly, quarterly and annual Security Reviews
2. Analysis and debriefing of Incidents that have occurred
3. Emerging trends from monitoring systems
4. Risk Management Committee meetings
5. Observation and reporting by staff members or contractors

In identifying risks, consideration shall be given to:

1. Internal and hosted systems used by the business
2. The Naverisk application provided to clients and its attendant systems and platforms
3. External vendors providing systems used for both internal use and in for the provision of the Naverisk application

4. Risks resulting from the action or inaction of staff or contractors, either accidental, deliberate or fraudulent.

11.0 Risk Management Committee

All risks identified must be reported to the Risk Management Committee. The Committee has scheduled meetings the first week of every month and bi-weekly. Once per quarter a further meeting is scheduled. In the event of a high risk being identified the Committee will hold an immediate Emergency Meeting. All meeting notes are recorded and a workflow process approved by all members.

The function of the Committee is:

1. Risk Identification
2. Risk Assessment
3. Risk Mitigation
4. Monitoring and Review of current risks
5. Recording of all risks and mitigations in the Risk Register

12.0 Risk Assessment

All identified risks are assessed to determine their likelihood of occurring, and the impact they would cause. From this the Risk Level can be determined using the matrix below.

	Consequences		
Likelihood	Minor	Moderate	Major
Unlikely			
Possible			
Likely			

Intolerable Risk Level Immediate action required
Tolerable Risk Level Risks must be reduced so far as practicable
Broadly Acceptable Risk Level Monitor and further reduce where practicable

All risks will be initially assessed to determine the Inherent Risk. This is defined as the initial risk level existing before any mitigating action is taken. Following mitigation, the risks are re-assessed to determine the new risk level resulting from the application of the mitigation. This is deemed the Residual Risk and shall be recorded in the Risk Management Register.

13.0 Risk Evaluation & Treatment

Each risk identified shall be evaluated to determine the actions required to mitigate the risks to an acceptable level. These actions can include

- the creation and application of policies or procedures
- changes to application code
- design or architecture alterations
- changes to vendors
- changes to agreed SLAs, and
- increased monitoring

Once determined, the mitigation actions shall be recorded against the applicable risk(s), and placed into application as soon as practicable. All data regarding Risk Evaluation is recorded fir auditing purposes.

All risks deemed to be of an intolerable level require urgent mitigation. Tolerable risks should be mitigated wherever possible; however, the Risk Management Committee may elect to deem these acceptable if no practicable mitigation is possible.

Appropriate monitoring or controls must be put into place for each mitigation to enable the efficacy of the mitigation to be assessed on an ongoing basis.

14.0 Communication and Consultation

All minutes and decisions of the Risk Management Committee must be communicated to the Senior Management team, Board of Directors or any other parties deemed necessary by the CEO.

All policies, procedures or other actions recommended as part of the mitigation must be communicated by the Risk Management Committee to all affected stakeholders and departments. These policies must also be attached as an addendum to the Risk Management Register.

15.0 Monitoring and Review

Appropriate monitoring is in place for all risks with Inherent Risks levels of Unacceptable or Tolerable. The form of this monitoring is determined and documented as part of the Risk Evaluation and Treatment process.

All risks are re-assessed each quarter as part of the Risk Management Committee meeting. The re-assessment must take into account the efficacy of the mitigating processes as well as changes to the internal and external environment that may impact the risk level.

16.0 Training and Awareness

All staff receive regular information on risk awareness, focussing on the identification of potential risks, and the correct procedures to report them. Any additional training is at the discretion of the Risk Management Committee.

In the event that new risks assessed as Intolerable are detected, awareness information will be provided to all relevant staff as soon as practicable.

Appropriate information on the mitigation policies, procedures or other changes that have been put in place will be provided to all relevant staff as soon as possible following any change.

17.0 Personnel Management

Naverisk has implemented a number of personnel management controls:

- All key employees that are responsible for developing and operating the platform are extensively interviewed for skills prior to hiring.
- Job requirements and responsibilities are documented in job descriptions, including skills and abilities, and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process.
- All new hires are subject to pre-employment background checks.
- Role-based security controls to limit access to parts of the system and maintain separation of duties as well as isolation of customer data.
- Staff violating security policies are subject to disciplinary action, up to and including termination of employment.
- Staff are required to immediately report potential security incidents and potential vulnerabilities to the highest levels of the company.

18.0 Physical Security and Environmental Controls

Naverisk's cloud service is hosted and operated from multiple data centre's operated by AWS, depending on the regional instance selected by the customer. These data centres are audited annually in accordance with the AICPA's Service Organization Control (SOC) framework.

The AWS data centres are highly-secure third party facilities and no Naverisk staff have access to these facilities.

19.0 Change Management

Naverisk has designed its Change Management Process to achieve these main service enhancement and improvement objectives:

- Rapid implementation of service enhancements and/or patches.
- No service disruption for users.
- Transparency, to ensure complete visibility to the specific changes being made.
- Accountability, to provide a clear audit trail of who is making the changes. This is complete using a workflow process so each step is signed off accordingly.

Each regional instance of the Naverisk platform is deployed using one instance that resides on two multi-server platforms supported by AWS for fail safe, redundancy and maximum up-time.

All source 'Master' code, versioning, code tracking, workflow management, and development are hosted in Atlassian Bitbucket.

Naverisk uses private repositories and standard tracking, versioning, and issue categorization features within Atlassian Jira and Bitbucket. These all require multi-factor user authentication, all code changes are recorded and published for visibility to the Development team. Access to these private repositories is granted exclusively by the Engineering team under the supervision of the Chief Technology Officer.

All development occurs solely on company-controlled computers. All code pushed to production is approved and tested, using peer reviews as considered necessary.

Write access to the production repositories is limited to the Change Approval team, applicable to each repository. Changes are made in forks or branches of the master repositories. When changes are complete, a pull request is submitted for approval to the Change Approval team. Approved pull requests are then merged into the master repositories by a member of the Change Approval team. Individual members of the Change Approval team are not permitted to approve their own changes; instead, such pull requests are submitted to and merged by one of the other Change Approval team members.

When enhancements or other changes are approved, the changes are automatically picked up by the build server in real-time. The build server proceeds with a clean installation of the new service, including installation

of all external dependencies. After the build is completed, a suite of automated unit and functional tests are run. Finally, a configuration management tool is used to deploy the final packages into production.

If a test fails, the build is interrupted, the changes are not deployed and the Engineering team is automatically notified of the failures. Changes that are deployed in production can be rolled back easily if an issue is found that was not detected by the automated test procedures.

Change requests received through Customer Support team also follow the standard change management process and are triaged for approval as a hotfix or tracked for inclusion in a future release.

Slack is used to facilitate and manage internal communications and documentation related to changes, security advisories, internally reported failures, incidents, and concerns, and service rollbacks.

20.0 Problem Management

Naverisk has implemented two distinct problem management systems.

- Externally reported problems are tracked in an online customer communication platform and managed by Naverisk Customer Success team until resolved.
- Internally, reported problems are tracked in the Jira issues system and follow the change management process for resolution. Externally reported problems may occasionally get linked to one or more internal issues when the resolution to the problem requires a change to the Naverisk platform components.

21.0 Data Backup and Recovery

Naverisk has implemented three distinct backup strategies to prevent the loss of any data:

- Mandatory use of company-approved, secure, cloud-based applications and repositories for daily operations and activities.
- Utilization of multiple third-party data centres to host and operate all modules of the Naverisk platform.
- Automatic replication of the databases to secondary data center, with periodic backups in the event that data corruption occurs and is not detected in a timely manner.

22.0 System Account Management

Naverisk's information resources encompass a variety of services and applications which are predominantly cloud-based and which utilize a variety of authentication mechanisms. In order to properly manage logical access in this environment, the company has implemented role-based security controls to limit and control access to all facets of internal IT and the online service.

The Chief Technology Officer manages and grants access to various employees to the primary components of the Naverisk platform as well as the development and testing environments of the live service.

The Human Resources team manages and grants access to employees, for general internal IT services including email and related services, file shares and other sales, general and administrative systems. For specific access the change management process is used.

23.0 Risk Assessment Process

Security risks are reviewed in context of change management in daily meetings, weekly operations and project reviews, as well as Senior Leadership team meetings.

Changes identified in security threats and risks are regularly reviewed and updates are made to existing control activities. Information security policies are performed as necessary.

Naverisk has placed into operation a risk assessment process to identify and manage risks that could affect the ability to provide reliable service to our customers. This process requires management to identify significant risks inherent in the provision of service to our customers and to implement appropriate measures to monitor and manage these risks.

The Risk Management Committee consists of high-level executives and is comprised of:

- Product owner
- Chief Executive Officer
- Chief Technology Officer
- Chief Information Security Officer

Naverisk has identified risks resulting from the nature of the services provided and implemented various measures designed to manage these risks. Risks identified include the following:

- Software defects associated with the software. For example, new bugs inadvertently introduced by staff while implementing enhancements to the system or patches of vulnerabilities.
- Failures or defects in the components utilized by customers to access the platform. For example, Content Delivery Network (CDN) outages or service degradation.
- Intentional acts initiated by either rogue staff or third parties. For example, denial of service attacks.

24.0 Information and Communication Systems

Naverisk has implemented a series of Security Policies and related protocols so that employees understand their individual role and responsibilities. This covers processing and controls to ensure that significant events are communicated in a timely manner. These include documented policies and procedures, the use of centralized communication systems (including live chat and email services) to communicate time sensitive

information, processes for security and system availability purposes that notify key personnel in the event of problems.

For inbound customer communications, the primary channel for customer communications is live chat from within the Naverisk platform that feeds directly into an online customer communication platform. Secondarily, and in cases where the platform may not be accessible, the support email address also feeds directly into the platform.

This platform is integrated with Naverisk at a detailed level so the company can communicate with customers individually, or in customer segments filtered by usage-level and/or service-type attributes. This service also provides a platform for inbound communication from customers with technical questions and/or other customer service issues.

In addition to the inbound communication channels described above, there are additional outbound channels for communication with customers. Customers are segmented by service type to ensure that outbound communications are only sent to relevant customers. This is the method used for several types of customer communications including:

- **System Changes and Enhancements.** Email notifications are sent out whenever system changes or enhancements are made. Part of the company's development and release strategy is to ensure that existing services are not adversely impacted by system changes and enhancements. Accordingly, these changes and enhancements are generally communicated after the changes are in production.
- Note, however, that changes that may result in incompatibilities to customers (a.k.a. "breaking changes") that are not the result of a vulnerability or security advisory are communicated in advance to affected customers.
- **System Failures, Incidents, Concerns and Other Issues.** Email messages are distributed to individual and/or segments of customers, as appropriate, notifying them of the issue and other relevant information.

25.0 System Monitoring

Naverisk has implemented steps for integrating information security and risk management processes to monitor systems directly and indirectly. Continuous monitoring enables the Engineering team and others to see a continuous stream of near real-time logs and snapshots of application security state, data, network, endpoints, and nearly all applications that have a direct or indirect impact to the system.

Naverisk has implemented an array of tools to monitor all aspects of the system, including but not limited to:

- Monitoring services and components.
- Server monitoring.

- Playing the role of a customer using services through end-to-end synthetic proxy transactions that simulate real transactions.

The company has integrated the alerts and alarms generated by these monitoring tools into its company-wide communications systems, proving a real-time view of system health and possible vulnerabilities.

Key incidents requiring further investigation or remediation are escalated to the Engineering team.

Additional monitoring occurs at a business level with the adherence to regular performance appraisals and enforcement of policies and procedures as a general practice.