# Apparisk Functional and Technical Requirements Document

**Version 1.0**

**May 8, 2015**

# 1. General Information

## 1.1 Purpose

The purpose of this functional and technical requirements document is to provide documentation to development team on the requirements to implement and operate on Safety Risk Management (SRM) solution.

## 1.2 Scope

This Functional and Technical Requirements Document will outline the functional, performance, security and other system requirements identified by SRM as the proposed information system solution for a Safety and Risk Management System.

# 2. Current System Summary

The Safety Risk Management solution does not currently have a single Cloud solution that integrates business processes seamlessly across the enterprise to deliver deep and broad visibility.

# 3. Functional Requirements

## 3.1 Summary of Functions

The SRM requires an innovative, single cloud based solution for a robust workflow and risk management system whose primary function is to:

- Expedite and streamline the process of delivery of service to company, Safety officer and auditor
- Transform the way companies manage safety risk management
- Help companies better analyze, manage and report safety risk information

### 3.1.1 Functional Requirements

- Authentication and Authorization
    - The system shall allow the user to login using email address or social login using OpenID (i.e. Facebook, Google plus).
    - The system shall allow the user to register their company either using email address or social login.
    - The system shall prohibit the unauthorized user to access to the system.
- Account and User Management
    - The System shall provide the unified user interface (henceforth referred as workspace) for users to access all the System's functionalities based on user's role and access right.
    - The workspace shall include the following
        - Dashboard
        - Administrative
        - Project Management
        - Workflow Management
        - Alert and Notification

- ▪ Certificate Management
- ▪ Worker Management
- ▪ Security
- ▪ Batch and Schedule Jobs
- ● The system shall allow following type of user role
  - ▪ System Admin
    - ● The system shall allow all system administrative functionalities to the user.
    - ● The system shall allow the user to approve or reject the registered company/ user against the terms and condition of the system
    - ● The system shall allow the user to rest the password for company admin.
    - ● The system shall send the email to the registered company/ user in terms of approval and rejection done by the admin user.
    - ● The system shall allow the user to add/ remove and the functionality from the system.
  - ▪ Company Admin
    - ● The system shall allow the user all company-level functionalities within their company.
    - ● The system shall allow the user to create the company staff or invite the user to the system.
    - ● The system shall allow the user to rest the password for company within the company
    - ● The system allow the user to give permission to company staff on some project or trade according to company business process.
    - ● The system allow the user to hire the safety consultant and auditor (i.e. third party who registered as safety consultant or Safety officer in the system).
  - ▪ Company Staff
    - ● The System shall allow the user to manage and monitor day to day risk management on assigned project or trade.
  - ▪ Safety Consultant
    - ● The System shall allow the user to manage and monitor day to day risk management on assigned project or trade on behalf of the company
  - ▪ Safety Auditor
    - ● The System shall allow the user to review and audit risk management done by company staff or safety officer on assigned project or trade.
- ● Administrative Module
  - ● The system shall allow to change the company profile
  - ● The system shall allow one only company admin for each company
  - ● The system shall allow to assign the company staff to company admin and system shall instantly demote the company admin to company staff and logout the system.
  - ● The system shall allow to reset password for company staff
  - ● The system shall allow to manage and monitor the user, worker, project and certificate.

- Project Management
  - The system shall show the list of project, trade or checklist to user.
  - The system shall provide the user to create, update the project, trade and checklist.
  - The system shall provide the unified user interface for project, trade or checklist.
  - The system shall allow the user to approve or rejects of the project, trade or checklist based on their user role and permission on the project.
    - There have three kind of role on the project.
      - Managed by - The user can give approval and rejection of the tasks and appointed to other user to manage, operate and audit the tasks.
      - Operated by - The user can prepare the risk assessment for the assigned tasks.
      - Audited by - The user can audit and give comment on the tasks
  - The system shall allow the user to track the progress or activity done on project, trade or checklist.
  - The system shall allow users to create the project or trade with wizard kind of interface.
  - The system will provide two workflows scenario to the system.
    - Top-down manner
      - The system shall allow the project owner to create all necessary trades and checklists and appoint the other user or company to conduct the risk assessment (RA) for them.
      - The system shall allowed the user (who managed the project or trade) to approve/reject RA.
      - The system shall provide the right to the user to close the project. After the project is close, the user cannot update anything on the projects
    - Bottom-up manner
      - The system shall provide the interface for users to submit their risk assessment to other company. The company shall consolidate all the risk assessment accordingly and approve/reject based on the submitted RA.
      - The system shall allow the company to appoint the auditor or submit to other company (upto project owner).
      - The system shall allow the project owner to close the project.
      - The system shall prohibit the user to edit on the closed project.
- Repository Management
  - File Management
    - The system shall allow the user to upload, delete the document to the system.
    - The system shall allow the user to overwrite the document with the same name attached to the same checklist.
  - Version Control
    - The system shall provide the user to keep different version of the file they upload/overwrite.
  - Project Plan Management

- ▪ The system shall keep the target safety certificated level together with their checklist which will help the user to save their time and effort for re-structure the checklist repeatedly.
  - ● Trade Management
    - ▪ The system shall keep trade together with their RA list which will help the user to consolidate all the RA for particular trade.
- ● Alert and Notification
  - ● General Notification
    - ▪ The system shall show users the notification of approval, rejection and assignment of tasks
  - ● Email Notification
    - ▪ The system shall send email to users regarding approval, rejection and assignment of tasks
- ● System Admin Module & Backend process
  - ● The system shall keep all activity done by the users within the system.
  - ● The system shall allow the user to reject and accept the registration of the company based on business rule and regulation.
- ● Worker Management (Manpower Management)
  - ● The system shall allow to save the worker information and their certificate.
  - ● The system shall notify the user the expiry of the certificate.
- ● Training Record Management
  - ● The system shall store all training attended by the worker.
- ● Reporting Module
- ● System Security
  - ● Integrated technical safeguards to ensure a high level of privacy and security, including
    - ▪ Back end server(s), including data encryption and transmission
    - ▪ Administrator controlled user name and password access
    - ▪ Automatic timeout/log-off
    - ▪ Administrator controlled user level read, write, edit and delete capabilities
    - ▪ Administrator controlled user level module and sub-module access
    - ▪ Automated audit trail
    - ▪ Information Security Industry Standard encryption and SSL certifications (currently 128-bit)
    - ▪ All technical safeguards required to be standard compliant
    - ▪ All security safeguards required for compliancy to the Data and Technical Standards

### 3.1.2 User Scenarios/Use Cases

Scenario 1: Main Con

Lucy is the project manager of company ABC. She handled the project X that must be compliance with BizSafe level 3. In this project, there have a lot of sub-con and they are doing their RA separately. After they finished RA, they submit RA to her. After receiving all RA from sub-con she need to

consolidate all the document, prepare the checklist, review one by one and give comment for approval and rejection. After that she submit to audit firm to audit.

She wants computerized system that she can create the project and the system will automatically create the checklist. After that she create the different trade for differ sub-con, the system will automatically created the relevant checklist and document, and she can assign to them. Sub-con will carry out the RA on assigned trade. When they have done, they notify her through the system. She approve or reject the submitted the RA via system so that sub-con will get the notification. If every RA is fine, she submit to auditor via system. The auditor will come into the system and audit the RA.

# 4. Performance Requirements

### 4.1 Accuracy and Validity

The system will employ numerous data quality assurance techniques, including but not limited to:

- Input masks
- Drop down lists with standard responses
- Record data completeness requirements
- Basic data logic warnings (i.e., Gender: Male with Pregnancy status: Y)

### 4.2 Timing

The system will be available online 24 hours per day, 365 days per week with the exception of scheduled and pre-notified system maintenance downtimes.

Data will become immediately available for use, both during input and for reporting unless otherwise negotiated with the hosting vendor. The hosting vendor will ensure that system resources are adequate for timely report generation response times and overall software functionality. The hosting vendor will ensure that system updates, software updates, and regular system maintenance is not completed during peak operation periods.

### 4.3 Capacity Limits

### 4.4 Failure Contingencies

In the event of a natural disaster, the hosting agency will ensure continuity of available by having adequate, tested disaster and recovery protocols and solutions in place that will facilitate minimal system availability. The hosting vendor will also ensure completion and validation of daily backups of both the client records and system structure.

# 5. User Interfaces