# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

**SECTION G5  
TEAM 7**

**SMART CONTRACT PRODUCT (SCP)**

**INCIDENT MANAGEMENT PLAN**

# 

# 

# 

# 

# 

# 

# 

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 9-3-2019 | 1.0 | Initial write-up | Kenny Kwek, Ong De Lin, Janell Lee, Mark Tan, Lau Jun Rong |
|  |  |  |  |

Table of Contents

[Revision History](#_bcpu8aolxur) **2**

[Introduction](#_ooo8dycikham) **5**

[Purpose](#_dj8ogl4f40xs) 5

[Goals](#_24zvel4vydy9) 5

[Critical-to-Quality (CTQs) & Key Performance Indicators (KPIs)](#_v52zs54r6abd) 5

[Roles and Responsibilities](#_eo1p9kv9jvl0) **6**

[IT Operations Manager](#_5v2dri2ua5u5) 6

[Support Manager](#_wos03jfdajqx) 6

[Tier 1 - Communication](#_8o0o4e7bu75k) 6

[Tier 2 - Business Analyst](#_z0r4tqt0lm9a) 7

[Tier 3 - Dev and Infrastructure & Security](#_shwxvnr6saer) 7

[Quality Assurance](#_12z56nqd1ucu) 7

[Incident Management Process](#_usjk5ykyc5pf) **8**

[Incident Definition Process](#_cojc8za0pr0g) 8

[Incident Identification](#_t0a1v0vd62id) 9

[Incident Logging](#_iyse32ix9ugr) 9

[Incident Categorization](#_s3qcjvvmlwkk) 9

[Incident Prioritization](#_9z7gxdqlcn8i) 9

[Incident Matrix](#_3va1l7gteoui) 10

[Incident Response Process](#_dlxz11hb1udc) 10

[Initial Diagnosis](#_efqh531ux272) 11

[Incident Escalation](#_h3tqzlqky8ty) 11

[Functional Escalation](#_l0k8xlms5v3z) 11

[Hierarchical Escalation](#_hyw2i0dyb5rl) 12

[Investigation and Diagnosis](#_aoqdti7mxwe2) 12

[Resolution and recovery](#_j47klojmh7t8) 13

[Incident closure](#_w5myak1zxiu3) 13

[Process Activities Breakdown](#_6ytyijaj7sp6) **13**

[Tier 1](#_5zxgvt5o1vi5) 13

[Tier 2](#_2augch2puchn) 14

[Tier 3](#_rz7oenghp2ka) 15

[Recovery Procedures](#_1vmeg5w98wk5) **15**

[When a port is down](#_o9ssl3v9ud88) 15

[When Google Slide has been attacked](#_b1pclejuahlu) 16

[When there is any corrupted files](#_npzklk5kaoil) 16

[When an emergency occurs](#_7q2eq6ophj8r) 16

[**Appendix**](#_ugjdyo6o5xe0) **18**

# 

# Introduction

## Purpose

The purpose of this document is to provide a general overview of the Incident Management Process. It includes Incident Management goals, objectives, scope, benefits, key terms, roles, responsibilities, authority, process diagrams and associated activity descriptions. This document is developed based on the ITIL framework.

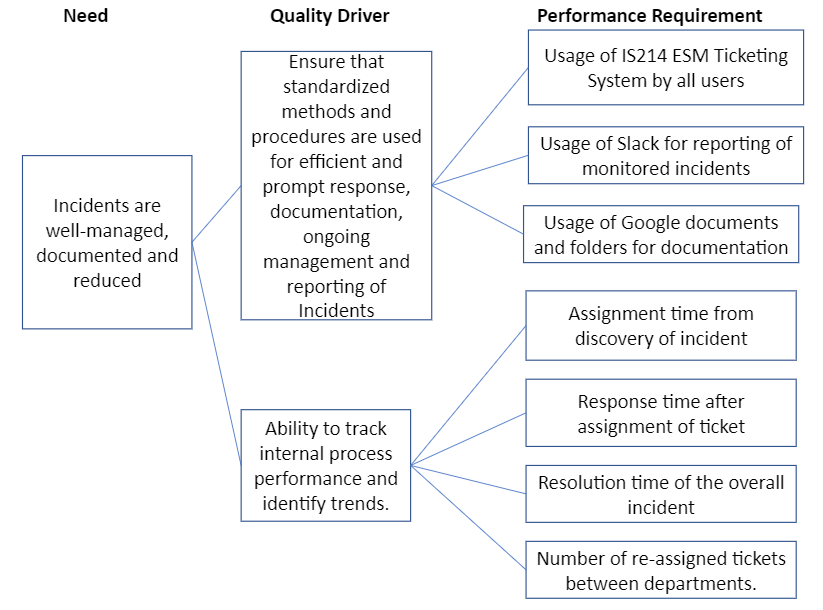
## Goals

The goals for the Incident Management process are to:

1. Restore normal operations in the shortest amount of time
2. Minimize the negative impact on business operations

## Critical-to-Quality (CTQs) & Key Performance Indicators (KPIs)

CTQs identified for the process of Incident Management and associated Key Performance Indicators (KPIs) are:



# Roles and Responsibilities

## IT Operations Manager

The IT Operations Manager is accountable for ensuring that the process is being performed according to the agreed and documented process and is meeting the aims of the process definition. He will report to the COO for any incidents.

The role includes responsibility for:

* Ensuring that the Incident Management process is fit for purpose
* Ensuring that proper Key Performance Indicators are set
* Ensuring that quality reports are produced, distributed and utilized
* Integrating the process into the organization
* Assisting with and ultimately responsible for the process design
* Defining appropriate requirements and standards to be employed throughout the process
* Documenting, training and publicizing the process including process changes
* Defining Key Performance Indicators (KPIs) to evaluate the effectiveness and efficiency of the process and design reporting specification
* Reviewing KPIs and taking the action required following the analysis
* Periodically auditing the process to ensure compliance to policy and standards
* Reviewing and initiating improvements in the tool, process, governance mechanisms and people

## Support Manager

The Support Manager is accountable to the IT Operations Manager. He performs the day-to-day operational and managerial tasks required by the process activities.

The role includes responsibility for:

* Document and publicize the process
* Define appropriate processes and standards for the process
* Ensure smooth operation of incident management resolution for Tier 1 to 3

## Tier 1 - Communication

Tier 1 - Communication will be at the frontline of the user support by communicating with the users who are reporting incidents. She will initiate, close and resolve tickets. She will escalate incidents which they cannot resolve to Tier 2 - Business Analyst. She is the main point of communication with users throughout the process

## Tier 2 - Business Analyst

Tier 2 - Business Analyst will monitor and track incidents. He will assign the incidents to Tier 3 - Dev and Infrastructure & Security for follow-up actions. He will determine the severity and whether incidents record requires special reporting. He will also investigates the nature and cause of incidents.

## Tier 3 - Dev and Infrastructure & Security

Tier 3 - Dev and Infrastructure & Security will investigate the nature and cause of incidents. He will resolve the cause of incidents and initiate change management process if incident requires one.

## Quality Assurance

The Quality Assurance will work alongside with the IT Operations Manager to define the KPIs to evaluate the effectiveness and efficiency of the process. He will also review opportunities to improve the efficiency and effectiveness.

# Incident Management Process

## 

## Incident Definition Process



The following overview table lists the RACI Matrix for the Incident Definition Process:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Activity** | **IT Ops Manager** | **Quality Assurance** | **Support Manager** | **Tier 1** | **Tier 2** | **Tier 3** |
| **Log, Categorize and Prioritize Incident** | I | C | A | R | C | I |
| **Update Priority** | I | I | I | R | C | I |

### Incident Identification

The main sources of potential incidents come from the following two areas:

|  |  |
| --- | --- |
| **Source** | **Channels used by source** |
| Users | Ticketing system |
| Alerts | FreshPing, Nagios, AWS Cloudwatch, Cloudtopus, VisualPing |

Of which, each issue that is derived from the above sources still need to be further identified to decide if they are indeed incidents. In the situation whereby the issue is a change request instead of an incident, it should then be sent through the change management process.

### Incident Logging

After an event is classified as an incident, it will be logged as per enterprise standard procedures. By logging the details, it helps to ensure that user information is accurate and ensures that this information is kept up-to-date to aid in categorizing or resolving the incident. As such, the incident log will include the following information:

* Ticket ID
* Name of issuer
* Contact
* Date Issued
* Category
* Sub-Category
* Steps taken before incident
* Has it happened before?
* Date and time of incident
* Date and time of resolution
* Status

### Incident Categorization

The incident will then be categorized into an appropriate category/subcategory, which helps to facilitate the automatic prioritization of some issues, the sorting and modelling of incidents and tracks incidents to monitor if any trends are found from the incidents.

### Incident Prioritization

Incident priorities are determined by their impact on users and on the business, as well as the urgency of how quickly a resolution is required to reduce the business impact. However, it should be noted that prioritization may change during the lifetime of an incident.

Our team will be using the following descriptions to determine the impact of an incident:

|  |  |
| --- | --- |
| **Impact** | |
| **High** | Affects a large number of users, interrupts business, or a group of VIPs. |
| **Medium** | Impacts a few users or an individuals, a few staff, or a VIP. |
| **Low** | Does not interrupt users or the business. |

Our team will be using the following descriptions to determine the urgency:

|  |  |
| --- | --- |
| **Urgency** | |
| **High** | Service delivery or core line of business is affected. |
| **Medium** | Interrupts work to some degree. |
| **Low** | Work remains unaffected. |

#### Incident Matrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Impact** | | | |
| **Urgency** |  | **High** | **Medium** | **Low** |
| **High** | Critical | High | High |
| **Medium** | Critical | High | Medium |
| **Low** | High | Medium | Low |

## Incident Response Process



The following overview table lists the RACI Matrix for the Incident Response Process:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Activity** | **IT Ops Manager** | **Quality Assurance** | **Support Manager** | **Tier 1** | **Tier 2** | **Tier 3** |
| **Initial Troubleshoot Using Knowledge Base** | I | I | A | R | C | C |
| **Combine similar requests/reports** | - | - | I | R | - | - |
| **Validate and accept incident** | I | - | A | I | R | I |
| **Reporting Per Priority** | I | C | I,C | I | R | - |
| **Use Existing Knowledge Base to begin Troubleshooting** | I | - | A,I | - | R | C |
| **Begin Incident Resolution** | I | - | A | I | I | R |
| **Determine if change is required to resolve incident** | C | I | C | - | - | R |
| **Complete incident resolution** | I | I | I | I | I | R |
| **Confirm incident status with user** | - | - | I | R | - | - |
| **Update Ticketing system** | - | I | I | R | C | C |

### Initial Diagnosis

In this step, actions will be taken by Tier 1 to diagnose the fault and, where possible, to resolve it at this stage. In order to do this, Tier 1 will be utilizing the Known Error database provided by problem management as well as any other diagnostic tools to assist in the diagnosis as well as the possible resolution.

In the case whereby Tier 1 is unable to resolve the incident, the initial diagnosis will be used to identify the appropriate support tier for escalation and prepare information of the incident to assist the second-tier of support in resolving the incident quickly.

As per ITIL guidelines, in such situations, Tier 1 will be using “incident matching” in which it is used to identify repeat incidents and the appropriate resolution steps ,by checking for previous incidents with the same classification.

*(Refer to Figure 1 for the overview of Incident Matching.)*

### Incident Escalation

Based on the ITIL framework, the team will be implementing two forms of escalation, namely functional escalation and hierarchical escalation, depending on the severity of the incident.

#### Functional Escalation

Functional Escalation takes place when the service desk is unable to resolve the incident and may be realized immediately depending on the type of incident or if Tier 1 has spent the maximum time allowed under the organization’s guidelines for attempting to resolve the incident without success. As such, it will be passed to the second-tier of support for resolution within a stipulated time limit for attempting to resolve the incident. If unsuccessful in resolution, it will proceed to be passed on to the third-tier of support. For each escalation, it will be accompanied by a Work Log documenting the actions taken by the previous support tier in their attempts to resolve the incident as well to facilitate the next support tier in resolving the incident.

However, occasionally it is clear to see that the incident will require a high level of technical knowledge, thus the incident will be immediately escalated without any attempt by the second-tier of support to resolve it. There may also be times where cooperation between different tiers of support is required or where the incident need to be referred to third parties such as software provision companies.

#### Hierarchical Escalation

Hierarchical Escalation takes place for high-priority or major incidents. It consists of communicating with the appropriate level of management about the incident so as to keep them within the communication circle and be consistently updated about the incident. By keeping the management informed, it will ensure that the management will be able to make decisions that are required, such as regarding prioritization of work, involving suppliers and more.

For major incidents, the IT Manager may be expected to brief the business directors about the progress of the incident or the business directors may approach the IT Manager directly, meaning it is vital for the IT Managers to have been comprehensively briefed themselves.

Additionally, in times when the progress of the incident is below the expected resolution speed, it could be necessary to conduct Hierarchical Escalation.

### Investigation and Diagnosis

After Tier 1 has undergone the initial diagnosis step covered earlier and ascertained that the incident can be resolved within Tier 1 themselves, this step will involve researching on what has happened and how the incident can be resolved by Tier 1.

For the purpose of investigations, a full description of the issue, its impact and urgency, a timeline of events, potential causes and the interrogation of knowledge sources such as the Known Error database will be carried out and documented.

As a part of the diagnosis, an incident report should also be created to record the actions attempted to resolve the incident, the actual actions taken to resolve the incident, description of the symptoms as well as actions required to prevent duplication of effort. As such, the collection of incident reports will be kept track of using the main incident log with the overview of all the incident reports.

Keeping track of the incidents will also be useful when the incident is reviewed during regular incident reviews, which will potentially play a crucial role in Problem Management.

### Resolution and recovery

After developing a potential incident resolution, it should be tested to ensure that it resolves the issue with no unintended consequences. Once the incident is resolved, it is Tier 1’s responsibility for closure.

### Incident closure

Once the incident is resolved and service has been restored, Tier 1 will contact the user to verify that the incident may be closed. By doing so, it would ensure that situations whereby the error appears resolved to the IT Support Team but is still affecting the user is avoided.

In situations whereby there are two incidents with certain overlapping symptoms, this will prove to be vital as the symptoms of one incident could be hidden by the other incident.

At this point, the category assigned to the incident should be reviewed again as the initial incident categorization could be inaccurate after gaining information of the verified cause.

However, in cases whereby the cause is still unknown after resolving the incident, a problem record may be raised to investigate the underlying cause and prevent any recurrences.

# Process Activities Breakdown

The following lists the activities carried out in the entire Incident Management process by the different tiers in the support team:

## Tier 1

|  |  |  |  |
| --- | --- | --- | --- |
| **Process activity** | **Description** | **Procedure** | **Metrics** |
| **Log, Categorize and Prioritize Incident** | Recording of the incident using the ticketing system to track and monitor the progress | * Incident logged into ticketing system * Include incident details * Incident is categorized * Incident is prioritized based on impact and severity | 1. Total number of incidents reported 2. Number of incidents by category 3. Number of incidents by priority |
| **Troubleshoot Using Knowledge Base** | Resolve incident ASAP if possible at the first point of contact to reduce impact | * Look through ticketing system to identify if similar incidents occurred previously * Use available knowledge to resolve the incident * Attempt to resolve the incident collaboratively with customer * Apply resolution if applicable | 1. Time to resolve incident 2. Incidents resolved using knowledge base |
| **Update Priority** | If multiple incidents of similar nature is reported, it may require escalation and additional resources | * Update priority of parent record based on impact and severity | 1. Number of high priority incidents |
| **Combine similar requests/reports** | Combine similar requests into one incident if there are multiple made. This reduces repeated and unnecessary resource usage to Tier 2 | - | - |
| **Confirm incident status with user** | Validation and confirmation of incident resolution with the customer | * Contact customer and request for confirmation on resolution of problem | 1. Length of time to closure |
| **Update Ticketing system** | Updating of the ticketing system on status for archiving and reference purposes | * Update ticket information and status and any information that contributed to the resolution | - |

## Tier 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Process activity** | **Description** | **Procedure** | **Metrics** |
| **Validate and accept incident** | Verify that incident is assigned correctly, correct priority, valid incident and acknowledged | * Review incident for validity * Acknowledges the acceptance | 1. Number of records incorrectly assigned Incidents 2. Number of tickets by priority 3. Time to assignment |
| **Reporting Per Priority** | Reporting of incident depending on severity and priority | * Determine if incident requires escalation to support manger * If yes, report to support manger | 1. Number of tickets requiring escalation |
| **Use Existing Knowledge Base to begin Troubleshooting** | Troubleshoot to find out the problem or root cause | * Check knowledge base for information on similar incidents * Begin troubleshooting | 1. Number of incidents troubleshooted |

## Tier 3

|  |  |  |  |
| --- | --- | --- | --- |
| **Process activity** | **Description** | **Procedure** | **Metrics** |
| **Begin Incident Resolution** | Take initial steps required to resolve the incident | * Begin investigating cause and problems * Take steps required to resolve the incident * If resolution requires assistance from a vendor or the acquisition or encounter complexity, inform support manager | 1. Number of incidents resolved 2. Time to resolve incident 3. Number of high complexity incidents |
| **Determine if change is required to resolve incident** | If change is needed to resolve incident, then a change management process must be initiated | * If change is required, inform support manager to request for change approval * Confirm that change request is approved | 1. Number of incidents that require change to resolve |
| **Complete incident resolution** | Take necessary steps to complete the ticket | * Updates information on the ticket * Assigns ticket back to Tier 1 | 1. Tickets with ‘resolved’ status |

# Recovery Procedures

## When a port is down

1. Verify that port is down by typing ‘ps -ef | grep :8000’ after accessing instance
2. If port is down, restart service by typing ‘nohup bash /home/ec2-user/Django\_Application/virtual\_env/ICA-1/ICA/bin/auto\_start.sh &>/dev/null &’
3. Repeat step 1 to check if port is open
4. If port is still down, restart instance from AWS console as last resort

## When Google Slide has been attacked

1. Access instance to verify
2. Access the directory of application’s startup file ‘cd /home/ec2-user/Django\_Application/virtual\_env/ICA-1/ICA/bin’
3. Temporarily replaced embedded google slide from “<https://docs.google.com/presentation/d/e/2PACX-1vRh_WpvKQ7K1CpV3LRSvwEOtYUXfqqlBYAFxIIij3sSZ-xbzlwLANUtaL6mgfccZWMvl_-aieKJQL4q/embed?start=true&loop=False&delayms=3000&slide=id.p>” to “<https://docs.google.com/presentation/d/e/2PACX-1vRh_WpvKQ7K1CpV3LRSvwEOtYUXfqqlBYAFxIIij3sSZ-xbzlwLANUtaL6mgfccZWMvl_-aieKJQL4q/embed?start=true&loop=False&delayms=3000&slide=id.p>"
4. Repeat step 1 to check whether google slide is updated

## When there is any corrupted files

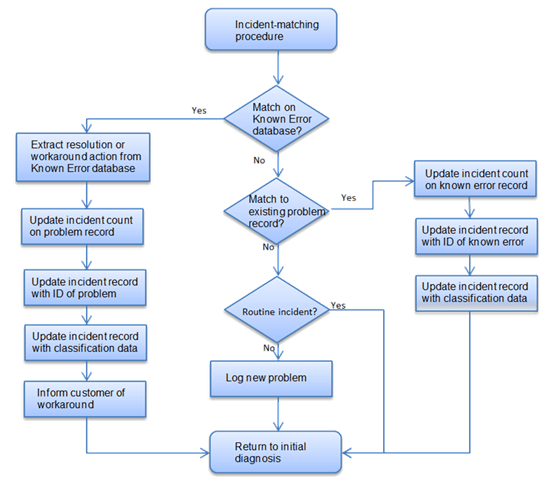
1. Stop instance
2. Detach current volume
3. Attach latest working AMI as current volume
4. Restart instance
5. Test that the application is working correctly
6. Check that there are no more corrupted files, else repeat Step 1 onwards

## When an emergency occurs

To temporary resolve the issue, we will replace the affected website application with a warm standby application. This ensures the end user will still be able to see the original content when logging into our URL ([www.esmscp.tk](http://www.esmscp.tk)). This is achieved through hosting a seperate copy of the application on a separate instance independent of the first. The steps are as follows:

|  |  |  |
| --- | --- | --- |
| **Steps** | **Actions** | **Details** |
| 1 | Host application on separate instance | Extract image of current working application and load it into the new instance |
| 2 | Test if hosted application is working as intended on the backup server | Access the URL and port address to ensure output is displayed correctly. |
| 3 | In the main instance and server, add a configuration line to redirect user to standby server in the event of an incident | Under nginx.conf, enter “Return 301 “http:x.xx.xx.xx;”. Test if the redirection is successful.  If yes, then comment out the line and take note to quickly enable the command in the event of an incident. |

# Appendix



*Figure 1 - Incident Matching (Based on Cabinet Office ITIL® material)*