Major Incident Management

Standard Operating Procedures

Company A Solutions Inc.

Confidential

Version 1.3

2025

Audience

This document is for the following audience:

- Company A support desk agents
- Company A internal stakeholders
- Company A IT
- Client IT
- Third-party vendors

References

- Server Down Process document
- Company A Support MI Escalation Process document
- Company A Services and Support Agreement document
- Company A Service Desk and Incident Management
- Company A ODOO Alerts Workflow Guide

Disclaimer

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of Company A Solutions Inc. (from now on, Company A). The information contained in this document is proprietary to Company A and may not be used or disclosed except as expressly authorized in writing by Company A.

Disclaimer

The electronic version of this document is recognized as the only valid version.

Contents

1 Overview 1

1.1 Purpose 1

1.2 Scope 1

1.3 Exclusions 2

2 Major Incident Management Process 3

2.1 Server Outages 6

2.2 Incident Severity Levels 7

2.3 Escalation Matrix 10

2.4 Service Level Agreement 11

3 Communication Playbook 12

3.1 Key Roles and Responsibilities 12

3.2 Communication Types and Guidelines 13

3.2.1 Internal Updates 13

3.2.2 External Updates (Clients) 13

3.2.3 Executive Briefings 14

3.3 Communication Channels 14

3.4 Email and Notification Templates 15

3.4.1 Initial Notification (Clients) 15

3.4.2 Progress Updates 16

3.4.3 Resolution Confirmation 17

3.4.4 Google Notification Template 18

3.5 Post-Mortem Review 18

4 Contact and Notification List 19

4.1 Company A Solutions 19

4.2 Customer Contact List 19

5 Important Links 20

6 Definition of Terms 21

7 Revision and Approval Record 24

1 Overview

This standard operating procedure (SOP) outlines the process for creating and managing a major incident ticket for service outages affecting Company A. This SOP includes instructions for initial reporting, notifications and updates, issue resolution, and root cause analysis (RCA).

1.1 Purpose

To create an efficient escalation notification channel for the IT Department and internal stakeholders during major incidents (MI). This process includes alerting and escalating server downtime notifications to IT and internal stakeholders, tracking incident management through ITIL-based procedures, and ensuring clients are informed of hosting service interruptions.

The SOP aims to maintain comprehensive coverage for major incidents and uphold ITIL best practices in a 24/7 environment.

- To mitigate service disruption by resolving the incident within the specified SLA.
- To minimize interruptions to normal operations.
- To limit the extent of disruption and damage.
- To establish a workaround for immediate solutions.
- To set a minimal service impact through rapid service restoration.

1.2 Scope

This procedure applies to major incidents and all personnel responsible for reporting and managing major service outages for the organization. A major incident is characterized by its Company Acant impact, especially on customers. Key characteristics include:

- Many customers or key customers are or will be affected.
- The cost to customers and/or the service provider is substantial, both directly and indirectly.
- The reputation of the service provider is likely to be damaged.
- The effort and time required to manage and resolve the incident are large, often breaching agreed service levels.
- Major incidents are usually categorized as critical or high-priority and are handled with greater urgency and shorter timescales.
- Company A-controlled major incidents: Company A is directly responsible for restoring services that impact external client systems.

- Client or third-party controlled major incidents: COMPANY A manages the incident but is not directly responsible for service restoration.

1.3 Exclusions

This Standard Operating Procedure (SOP) for creating and managing a major incident ticket for Company A specifically excludes the following:

Exclusions	Details
Non-Major Incidents and Service Requests	This SOP does not cover procedures for handling minor incidents or routine service requests. This is managed through standard support channels and procedures.
Non-Company A Services	The procedures outlined in this SOP are exclusive to service outages affecting Company A technology and do not apply to incidents involving services or systems outside the Company A infrastructure.
Post-Incident Review and Reporting	This SOP does not include detailed steps for conducting post-incident reviews or generating post-incident reports. Separate procedures exist for these activities, which will occur and be closed within 1 week of the event.
Emergency Situations	In cases where immediate action is required to mitigate severe risks to safety, security, or critical business functions, this SOP may be bypassed in favor of emergency protocols established by the organization.
Events Under 15 Minutes	This SOP excludes incidents or service outages that are resolved within 15 minutes. These brief interruptions will be documented and handled through standard support procedures. Company A will still communicate the event occurrence and resolution in real time.
Long-Term Process Improvements	This SOP does not cover long-term changes to processes or infrastructure aimed at preventing future incidents. These improvements are managed through continuous improvement and change management processes.

2 Major Incident Management Process

A major incident (MI) is the highest impact category for an incident, causing Company Acant business disruption. Major incidents are not always P1 issues; P2, P3, or P4 issues can also be classified as MIs based on their business impact.

- **COMPANY A Major Incident**: Incident for which COMPANY A is directly responsible for the restoration of services, which impact external client systems.
- **Client or 3rd party controlled Major Incident**: Incident for which COMPANY A is not directly responsible for restoration of impacted services but is responsible for managing the Incident to resolution.

The incident management workflow consists of steps to effectively detect, respond to, mitigate, and resolve incidents. This includes initial detection, alerting stakeholders, and promptly communicating with support teams and management.

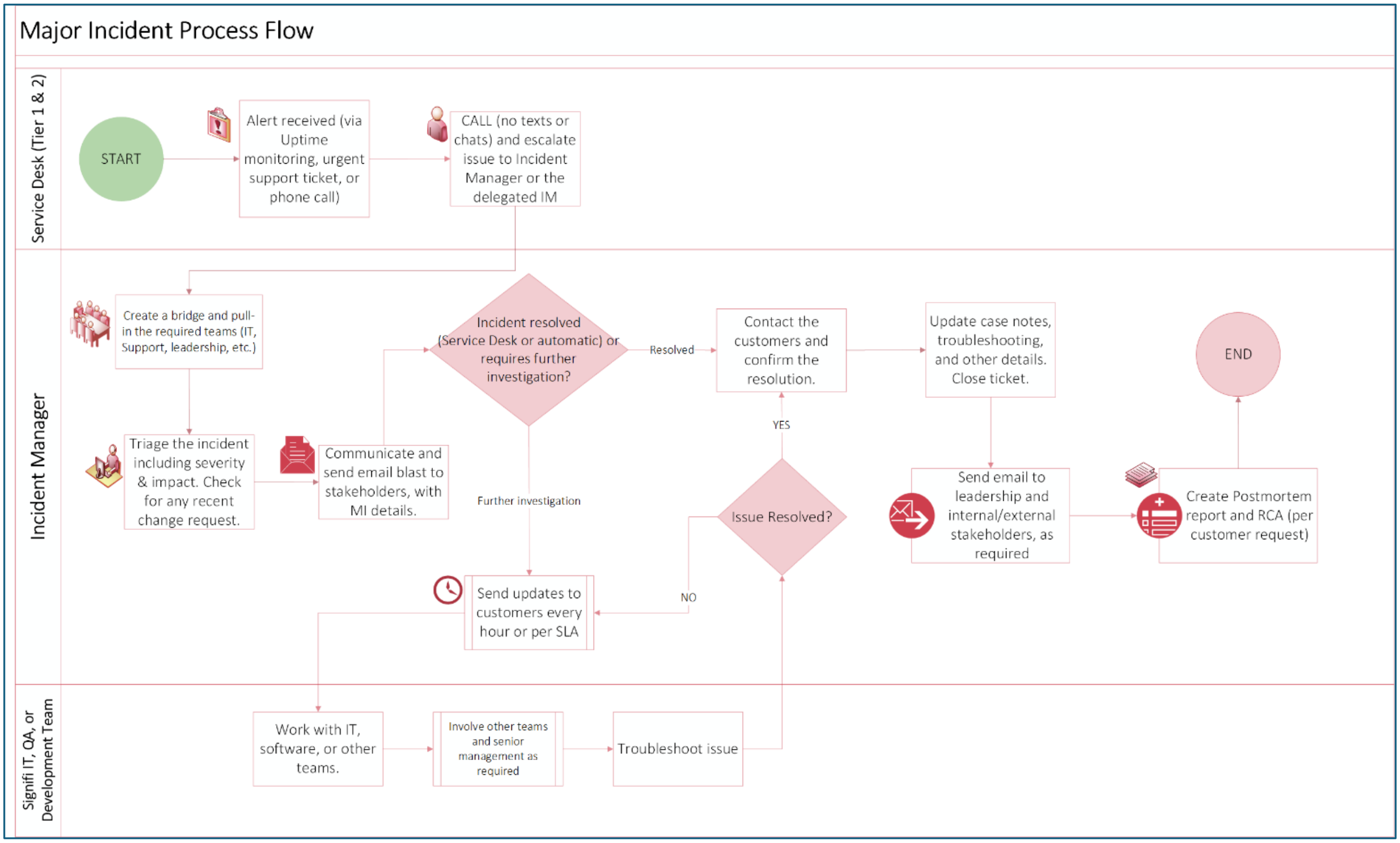

Major Incident Process Flow
Service Desk (Tier 1 & 2)
START
Alert received (via Uptime monitoring, urgent support ticket, or phone call)
CALL (no texts or chats) and escalate issue to Incident Manager or the delegated IM
Incident Manager
Create a bridge and pull-in the required teams (IT, Support, leadership, etc.)
Triage the incident including severity & impact. Check for any recent change request.
Communicate and send email blast to stakeholders, with MI details.
Incident resolved (Service Desk or automatic) or requires further investigation?
Resolved
Further investigation
Contact the customers and confirm the resolution.
YES
Issue Resolved?
NO
Send updates to customers every hour or per SLA
Update case notes, troubleshooting, and other details. Close ticket.
Send email to leadership and internal/external stakeholders, as required
Create Postmortem report and RCA (per customer request)
END
Signifi IT, QA, or Development Team
Work with IT, software, or other teams.
Involve other teams and senior management as required
Troubleshoot issue

Figure 1 Major Incident Process Diagram

Follow this process to manage major incidents:

1. An alert is created through one of the following sources:
   - Uptime monitoring
   - Phone call
   - A support ticket marked as **Urgent** or *upgraded* to **Urgent**.
2. The Support team immediately calls the Incident Manager (IM) to escalate the issue.

📝 If the IM is on leave, their delegated IM or direct manager will take over the duties.

3. The Incident Manager creates a calendar call and then opens a bridge (in Teams) involving the following persons:
   - Phone or WhatsApp call to Company A's **CCO Henry Hey (416-460-8684)**
   - Phone or WhatsApp call to Company A's **IT Director** or **Support Services Director**
   - Company A senior management/leadership team (as necessary)
   - Subject Matter Experts
   - External clients (if required)

📝 If a major incident occurs after hours, the Support Agent must Call the IM to address the event.

4. The IM and Support team triage the incident, assessing its **severity** and **business impact**.
   - Check **how many units are affected** and whether **other customers are affected**.
   - Review **any recent changes, completed change requests,** or **scheduled maintenance**.
   - **Case notes should be updated** with triage findings. Refer to this MI ticket as an example: https://Company Asolutions.odoo.com/web#id=1772261&menu_id=304&cids=1&action=417&active_id=1&model=helpdesk.ticket&view_type=form
   - Ensure proper ticket coding including **System**, **Component**, **Problem Code**, **Software Version**, etc.
5. The IM sends out an incident notification to internal and external stakeholders using the Email Marketing App in Odoo. Refer to the Email and Notification Templates for samples.
6. If the incident *resolves on its own*, the IM and Support team should update the case notes with resolution details and all troubleshooting steps performed. The IM must:
   - Contact affected customers to confirm the resolution
   - Notify internal stakeholders
   - Prepare a post-mortem report and RCA if required.

7. If the issue is ongoing, the IM must send status updates to affected customers every hour or as required by the SLA.
8. The IM coordinates with IT, software, or other relevant teams throughout the troubleshooting process. Senior management may be involved in communications if necessary.
9. The IM follows up with the relevant team and continues to update customers every hour or according to SLA terms until the resolution is confirmed.
10. If a Disaster Recovery (DR) plan is required, IT declares a DR event and initiates the recovery process with the designated DR partner.

📝 IT must inform the IM and Support group once DR has been activated.

11. Once the *issue is resolved*, the IM confirms the resolution with customers, updates the case notes, and provides a full summary of the incident, including all steps taken and outcomes.
12. The IM sends a closure email to leadership, internal stakeholders, and affected clients, as required.
13. The IM (for external issues)or IT Team (for internal issues or maintenance) prepares a post-mortem or Root Cause Analysis (RCA) report if required. This includes all relevant case notes, findings, and lessons learned.

📝 It must be delivered within 7 business days (168 hours, excluding weekends), though this timeline may be extended depending on incident severity and involvement of third parties

For more information, see Contact and Notification List, Email and Notification Templates, Escalation Matrix, KPI and Service Level Agreement

2.1 Server Outages

A managed Disaster recovery as a service (DRaaS) is implemented with CTC (Canadian Tire), as part of the hosting plan known as **Option B**, to protect the cloud-based Vision platform hosted at Company A's partner, Simnet, in the Toronto managed data center.

The target environment for these VMs will be Simnet DR servers in Montreal, QC, Canada. The technology stack is designed to achieve a 15-minute RTO/RPO for DR failover.

There will be one DR test drill per year for all affiliates combined. These drills will last a maximum of 4 hours and require 2 weeks' notice on a mutually agreed-upon date.

Company A will execute their full regression test suite, followed by CTC executing their regression test suite. The DR failover needs to be automatic from the lockers, rather than manual failover.

The goal of disaster recovery for enterprise deployments is:

- To minimize interruptions to normal operations.
- To limit the extent of disruption and damage.
- To establish alternative means of operation in advance.
- To provide for smooth and rapid restoration of service.

Exclusion to the process is on evenings that Company A server scheduled maintenance occurs. See Calendar (https://Company Asolutions.sharepoint.com/sites/Company AIT/Lists/Events/calendar.aspx)

The disaster recovery plan assumes that Company A employees are not affected by the disaster and can carry out disaster recovery activities. Staffing, training, relocating employees to carry out disaster recovery in an alternate city/region is beyond the scope of this disaster recovery plan. (Force Majeure).

2.2 Incident Severity Levels

The list defines the incident severity levels. Refer to the table below for more information.

P1: Critical

- The service is severely impacted or there is widespread client impact.

P2: Major

- Major functionality is impacted, affecting several clients. Service is limited with partial interruptions.

P3: Minor

- The service is functional, but it experiences periodic errors or non-critical malfunctions.

P4: RFO

- Technical questions, clarifications, and inquiries regarding the reason for the outage.

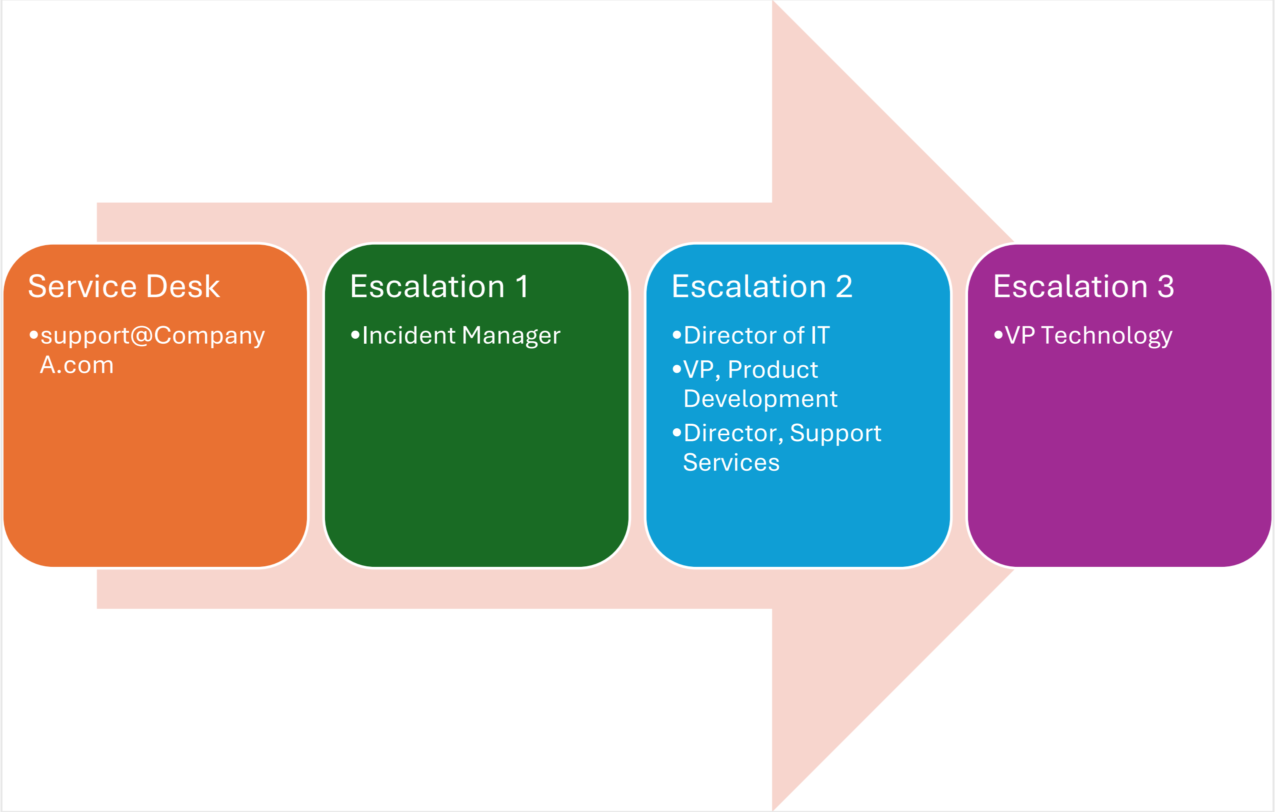
Priority	Examples	Actions to be Taken
P1 (Critical and Urgent) The entire service is down or there is widespread client impact.	• Service is completely down or severely impacted in multiple locations. • Revenue or dispensing is affected. • Multiple kiosks are logged out.	• **Immediate escalation** to Services Director, IT Director, Leadership, and Executive Sponsors. • Immediately send an initial notification. • Provide ongoing updates and proactive communication. • Triage the incident. • Contact the site POC and attempt a remote fix or temporary workaround. • If unresolved, escalate and dispatch onsite support.

Priority	Examples	Actions to be Taken
P2 (High) Major functionality is impacted, affecting several clients. Service is limited with partial interruptions.	• Partial dispensing issues (e.g., one or more lanes fail, but the kiosk still operates). • Camera malfunction. • One or two doors fail to open via software.	• Escalate to the IT Team Lead and Account Managers. • Provide ongoing updates and proactive communication. • Diagnose the issue and identify root causes for immediate triage. • Implement temporary workarounds while working on a fix. • If unresolved, escalate to higher support levels. • If remote resolution isn't possible, dispatch onsite support. • Provide ongoing updates and proactive communication.
P3 (Medium) The kiosk is functional, but it experiences periodic errors or non-critical malfunctions.	• UI errors (kiosk still dispenses and processes transactions). • Non-critical malfunctions. • Minor errors.	• Alert the Support Team. • Identify root causes and determine a fix. • Resolve remotely if possible; otherwise, assess the need for onsite dispatch. • Provide updates as they become available.
P4 (Low) Cosmetic issues, minor impacts, or general inquiries.	• Vinyl damage. • Planogram change requests. • UI text changes. • Training requests or procedure clarifications.	• Assist the customer with commercially reasonable efforts. • Assign tasks to the appropriate team.

Priority	Examples	Actions to be Taken
		• Assess and coordinate necessary improvements with the customer. • Provide updates as they become available.
Service Requests **Tasks that are not service failures but scheduled or routine requests.**	• Reporting requests. • IMAC (Install, Move, Add, Change) requests. • Configuration change requests.	• Assign tasks to the appropriate team. • Provide scheduled dates and updates at a logical cadence.

2.3 Escalation Matrix

The Service Desk agent initiating the escalation must speak directly with the Incident Manager or the next escalation point via phone or Teams; text messages are not allowed.



Service Desk
- support@Company A.com

Escalation 1
- Incident Manager

Escalation 2
- Director of IT
- VP, Product Development
- Director, Support Services

Escalation 3
- VP Technology

Here's the detailed escalation process:

1. **Initial escalation** to Incident Manager (IM).
   - The first point of contact for L1 support when an issue needs to be escalated is the **IM**.
   - The L1 support should provide the ticket number and other information about the issue.
2. **Secondary escalation** to the Director of Support, Director of IT, or Director of Product Development.
   - If the IM does not respond within 5 minutes, the issue should be escalated to the Director of Support or Director of IT.
   - Include the ticket number and other information about the issue.
3. **Tertiary escalatio**n to the VP of Technology.
   - If there is no response from the Director of Support or Director of IT within an additional 10 minutes, escalate the issue to the **VP of Technology**.
   - Provide the ticket number and a comprehensive summary of the issue.

For more information, see Major Incident Management Process and Contact and Notification List

2.4 Service Level Agreement

This section describes the service level agreements (SLA) for common incidents.

KPI	SLA
Send communication blast to impacted stakeholders	**Immediately** or within **15 minutes**
Response time for service desk	**Immediately** or within **15 minutes**
Response time to IT	**Immediately** or within **15 minutes**
Updates sent to clients	Every **1 hour**, regardless of whether updates are available or not.

Recovery Time Objective (RTO)	P1 = **2 hours**
	P2 = **4 hours**

Recovery Point Objective (RPO)	P1 = **2 hours**
	P2 = **4 hours**

Post-mortem and root cause analysis	Minimum of **7 days** or **168 hours**

For more information, see Escalation Matrix

3 Communication Playbook

This playbook ensures clear, timely, and consistent updates during incidents. This communication playbook applies to all incidents and aims to:

- Inform stakeholders promptly and accurately.
- Share actionable updates based on the incident's status
- Protect reputation and maintain client trust.
- Coordinate internal teams for updates and faster resolution.

3.1 Key Roles and Responsibilities

Role	Responsibility
Incident Manager	Oversee incident communication and ensure updates are per the timeline.
IT Director	Provide technical details about the incident cause, progress, and resolution steps.
Support Lead	Coordinate updates related to customer impact and recovery efforts.
Account Manager	Communicate directly with affected clients, ensuring alignment with internal updates.
Executive Sponsor (John Martin)	Approve external communications for high-priority incidents.

3.2 Communication Types and Guidelines

3.2.1 Internal Updates

Audience	**Internal teams such as IT, Support, Service Delivery Managers, Account Managers, Leadership**
Frequency	**Immediately** or within **15 minutes**. Send an update every **1 hour**, regardless of whether updates are available or not. See the **Service Level Agreement**
Content	• **Incident status** (e.g., "investigating," "mitigating," "resolved"). • **Key updates**: findings, actions taken, and next steps. • Any **blockers** requiring escalation.
Communication Channels	Email updates, Teams channel updates, or call bridge.

3.2.2 External Updates (Clients)

Audience	Affected clients and other stakeholders
Frequency	**Immediately** or within **15 minutes**. Progress updates: send an update every **1 hour**, regardless of whether updates are available or not. See the **Service Level Agreement**
Content	• **Incident Overview** (brief and non-technical) • Current **impact** on services. • **Key updates**: findings, actions taken, and next steps. • **Estimated time** for the next update.
Communication Channels	Email templates, client portals, or direct calls for high-priority clients.

3.2.3 Executive Briefings

Audience	Company A Leadership and high-level stakeholders
Frequency	Tailored to incident severity. See the **Service Level Agreement** for additional information.
Content	• Incident Overview • Current **impact** on services. • **Key updates**: findings, actions taken, and next steps. • Event log and timestamps • Financial or reputational risks. • Recovery strategy and mitigation steps.
Communication Channels	Teams bridge calls or emails.

3.3 Communication Channels

Channel	**Purpose**
Email	Formal updates to clients and leadership.
Teams	Real-time communication among internal teams.
Client Portal	Posting status updates and resolutions for client access. (WIP)
Incident Hotline (1-877-744-6434, option 2)	Dedicated phone line for urgent client inquiries during incidents.

3.4 Email and Notification Templates

When a major incident occurs, timely client communication is essential. The incident manager is responsible for sending three key updates:

- Initial notification/email blast
- Progress updates based on SLA requirements
- Final resolution confirmation

These communications can be sent via the **Odoo Email Marketing** app or your Company A email. Several templates are available for use in the Email Marketing app. This chapter provides email templates and examples from previous incidents to guide your communications.

3.4.1 Initial Notification (Clients)

Email Fields	Content
Subject	**Incident Notification - [Service Impact]**
Body	Dear [Client Name], We are writing to inform you of an incident affecting **[specific services/kiosks]**. Our team is actively investigating the issue and working toward a resolution. • Incident Start Time: [Timestamp] • **Impact**: [Brief description of client impact] • **Next Update**: [Estimated time] We apologize for the inconvenience and appreciate your patience as we address this matter. Best regards, [Your Name] [Your Position] Company A Solutions [Your Contact Information]

3.4.2 Progress Updates

Email Fields	**Content**
Subject	**Incident Update - [Service Impact]**
Body	Dear [Client Name], We wanted to provide an update regarding the ongoing incident. Our team has identified **[brief description of findings]** and is taking the following actions: • **Current Status:** [Investigation/Mitigation/Resolution phase] • **Actions Taken:** [Key steps completed] • **Next Steps:** [Planned actions and timeline] • **Next Update:** [Estimated time] Thank you for your understanding. Please reach out if you have any concerns. Best regards, [Your Name] [Your Position] [Your Contact Information] **Company A Solutions**

3.4.3 Resolution Confirmation

Email Fields	**Content**
Subject	**Incident Resolved - [Service Restored]**
Body	Dear [Client Name], We are pleased to inform you that the incident affecting [specific services/kiosks] has been resolved. The service has been restored as of [timestamp]. • Incident Start Time: [Timestamp] • Resolution Time: [Timestamp] • **Root Cause:** [Brief description] • **Preventative Measures:** [Steps being taken to prevent recurrence] We sincerely apologize for any inconvenience caused and thank you for your patience. Best regards, [Your Name] [Your Position] [Your Contact Information] **Company A Solutions**

3.4.4 Google Notification Template

Fields	**Content**
Subject	(Sample) Major Outage – Stuff Station, Grab and Go, Vision Server
Body	• **Summary of Services Down:** For example, Google Vision instance for stuff station and Grab and Go was down again, and it is showing bad gateway/protocol. While it is down, the user's experience will show that the UI is not responding and will be stuck on a white screen. • **Localization**: For example, *AMER, EMEA, LATAM or global*. • **Occurrence**: For example, *11:30 AM EDT* • **ETA for Resolution**: Provide if available; otherwise, state *Unknown*. • **Additional Contact Info**: Provide any relevant contact details. • **Odoo ID**: Include the ticket ID for reference. • Status: Resolved, Open, etc.

3.5 Post-Mortem Review

- Schedule a debrief within 48 hours of resolution.
- Produce an RCA if required.
- Prepare the root cause analysis if required.
- Gather feedback on communication effectiveness.
- Update the playbook based on lessons learned.

4 Contact and Notification List

Use the details provided below to get the contact information and notification list for each company.

4.1 Company A Solutions

Contact Name	Email	Contact Via

4.2 Customer Contact List

Use this list or Odoo to get the comprehensive contact list:

5 Important Links

- https://Company Asolutions.freshdesk.com/support/login

6 Definition of Terms

Definition of terms used in this document.

Term	Definition
Change Management Processes	The methods and procedures used to manage changes to IT systems.
Contact and Notification List	A list of contact information for individuals and teams to be notified during incidents.
Disaster Recovery as a Service (DRaaS)	Disaster Recovery as a Service (DRaaS) is a cloud computing service model that enables an organization to back up its data and IT infrastructure in a third-party cloud environment.
Disaster Recovery Plan (DR)	A set of procedures to recover and protect a business IT infrastructure in the event of a disaster.
Downtime	A period during which a system is unavailable or inoperative.
Escalation Notification Channel	A communication pathway used to notify and escalate issues to higher authorities or stakeholders.
First Responder	The individual who first identifies and reports the major incident.
Freshdesk	A support software used to create and manage incident tickets.
Freshstatus	A status page service used to communicate the status of incidents to customers.
Incident	An unplanned interruption to an IT service or reduction in the quality of an IT service.
Incident Management Process	The workflow and procedures involved in managing and resolving incidents.
Incident Manager (IM)	The Incident Manager is responsible for overseeing and managing the incident response process.

Term	Definition
Incident Severity Levels	Categories that define the impact and urgency of an incident.
Initial Reporting	The first step in the SOP process where an incident is reported.
Issue Resolution	The actions taken to solve the problem causing the service outage.
ITIL	Information Technology Infrastructure Library, a set of detailed practices for IT service management.
Key Performance Indicator (KPI)	A measurable value that demonstrates how effectively an organization is achieving key business objectives.
L2 Incident Manager (IM)	Level 2 Incident Manager – Member of the Major Incident Management team acting on behalf on the Service Desk which acts as information distributor to various areas of business during a Major Incident.
Major Incident (MI)	A major incident (MI) is the highest category of impact for an incident, which results in Company Acant disruption to the business. Major incidents are not always a P1 issue, as P2, P3, or P4 issues are capable of being a Major Incident (MI) dependent on business impact to the organization.
Major Incident Management Team (MIMT)	Responsible and accountable for the resolution of the Major Incident.
Major Incident Ticket	A documented record used for reporting and tracking Company Acant service outages affecting Company A.
Notifications and Updates	The process of informing relevant stakeholders about the status and progress of an incident.
Post-Incident Review	An analysis conducted after an incident to understand its causes and effects.
Postmortem	A report created after a major incident to analyze what happened and identify measures to prevent similar incidents in the future. This report is created in conjunction with the Root Cause Analysis (RCA).

Term	Definition
Recovery Point Objective (RPO)	The maximum acceptable amount of data loss measured in time.
Recovery Time Objective (RTO)	The maximum acceptable amount of time to restore a system after a disruption.
Root Cause Analysis (RCA)	This is used to identify the underlying reasons for the major incident.
Service Level Agreement (SLA)	A commitment between a service provider and a client on the expected level of service.
Company A	Company A Solutions Inc
Standard Operating Procedure (SOP)	A detailed, written set of instructions to achieve uniformity in the performance of a specific function.
Tier 1 and Tier 2 Support	Levels of technical support with varying degrees of expertise and responsibility.
Uptime	The time during which a system is operational and available for use.

7 Revision and Approval Record

If this document requires revision, contact the document owner. The document owner shall contact the relevant groups to update this document.

Version	Date	Summary	Authors	Reviewers and Approvers
1.0	2024 July	Consolidated information from other process documents.	• Adrian D. •	•
1.1	2025 Jan 13	Revised MI process diagram	Adrian D.	
1.2	2025 Feb 03	• Added Chapter 3, Communication Playbook • Updated Chapter 5, Email and Notification Templates	Adrian D.	
1.3	2025 April 09	• Enhanced diagram and workflow to include additional scenarios • Emphasized escalation protocol: phone calls required (no text/Teams chat) • Added incident triage requirements based on severity and impact	Adrian D.	