TLP:WHITE = Disclosure is not limited

Notification Management

DSOP Control Information Common Standard - Operational processes

V 2.0

Change Log

Version	Change description	Approved by
2.0	Approved version	Referansegruppe Bank

Glossary

Term	Norwegian	English
Notifier	Sender av meldingen	The sender of the notification
Receiver	Mottaker av meldingen	Recipient of the notification

Notification Management

Preconditions for notifications

- Notifications are sent if a service experiences downtime, is not accessible, is taken offline for maintenance, or if unforeseen events lead to the service being inaccessible.

- The financial institution must deliver the notification by email to varsling.kontoopplysninger@list.bits.no.
  - This e-mail address redistributes the notification to Bits and the public agencies that use the service.

- The public agencies must ensure that they are able to receive notifications by email from varsling.kontoopplysninger-owner@bits.no.
  - Public Agencies are required to register at least one recipient of notifications and to inform Bits of any changes in the recipient address.
  - Bits will inform public agencies if there are any changes to the notification channel.

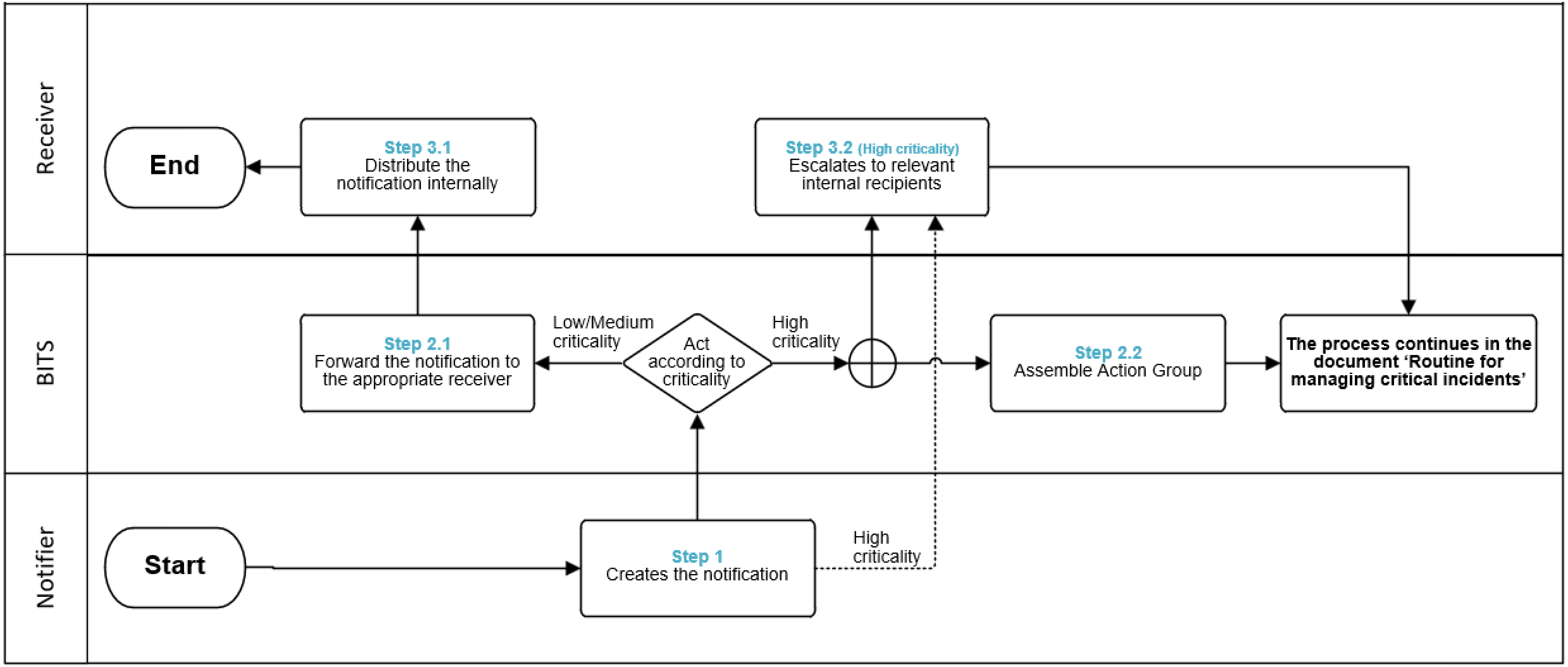
Notification Management

When should a notification be sent?

- If the service is unavailable, provides less information than expected, or when other relevant information that may impact the service arises. Examples of when the financial institution should send a notification includes, but are not limited to:
  - Maintenance
  - Downtime
  - Deviations and errors with planned fix
  - Changes

- The financial institution must send a notification when a deviation or error is detected and when it is resolved. This requirement also applies to planned changes and their deployment. Notifications should be sent at each step, even if the financial institution has already informed Bits in advance.

Notification Management Process



Receiver

BITS

Notifier

Start

Step 1
Creates the notification

Act according to criticality

Low/Medium criticality

Step 2.1
Forward the notification to the appropriate receiver

Step 3.1
Distribute the notification internally

End

High criticality

Step 3.2 (High criticality)
Escalates to relevant internal recipients

Step 2.2
Assemble Action Group

The process continues in the document 'Routine for managing critical incidents'

Step 1.

The *Notifier* should consider the following when creating the notification

- The notification does not need to be completely standardized since the public sector will receive it via e-mail. To ensure the notification contains sufficient information, the following should be included:
  - NotificationID (unique internal identifier). This is set by the financial institution. The purpose of this is for public sector and Bits to refer to the notificationID when they need to contact the financial institution regarding this issue.
  - Solution: Control information (Accounts API, Account list API, Transactions API, Roles API or Cards API)
  - Service: Konkursbehandling, Vergekontroll etc.
  - Category: Maintenance, downtime, deviations, changes
  - Environment: Test or production
  - Description
  - Date and time for incident and/or time for planned maintenance/downtime/fix/change
  - Status

- Additional relevant information can be included as needed. The examples listed above are not exhaustive. If the existing categories do not apply, you can opt for a different category that fits better.

- In cases of a high criticality notification, the Notifier will send the notification to both Bits and directly to the *Receiver*.
  - The contact details can be found in Appendix 3 of the agreement “SLA og varslingsrutine” – chapter 2.7.1.

Step 2.1 and 2.2

Bits forwards the notification to the Receiver

- **Step 2.1**
  - Bits forwards the notification to the appropriate receiver when low/medium criticality.

- **Step 2.2**
  - If the criticality is high, Bits assembles the Action Group in accordance with appendix 3 of the agreement - "SLA og varslingsrutiner" – Chapter 2.4.3.

Step 3.1 and 3.2

The Receiver of notification

- **Step 3.1**
  - The *Receiver* must distribute the notification to relevant parties internally.

- **Step 3.2**
  - The *Receiver* must distribute the notification about high criticality to relevant parties internally.
  - The *Receiver* awaits further information from Bits, who will assemble the Action Group.

DSOP

DIGITAL SAMHANDLING OFFENTLIG PRIVAT