BNP, Inc.
Bankers New Paradigm

Incident Response Playbook

Commercial Loan Origination during an outage of Email (Microsoft 365 Exchange Online). Illustrative example built from anonymized BIA records.

Item	Detail
Client	Example Community Bank
Department	Commercial Loan Origination
Resource	Email (Microsoft 365 Exchange Online)
Scenario	Email fully unavailable for up to 48 hours, the shortest maximum tolerable downtime among the dependent functions. Telephones, the loan origination system, the core and the internet remain available.
Version	0.1
Prepared	November 13, 2026, by BNP, Inc.
Status	Draft for department review

1. Purpose and Scope

This playbook sets out what the Commercial Loan Origination department does to keep loans moving while email is unavailable, from the first sign of an outage until the backlog is cleared. It covers one resource and every origination function that depends on it, in priority order. Use it whenever Outlook or Exchange Online cannot send or receive mail for the department, whether the cause is a provider-wide outage, a tenant problem or a cyber event. It does not replace the Bank's IT incident response plan or Microsoft's recovery of the service; restoring a hosted mail service is the provider's task, and this playbook covers how the department continues its work while that happens.

This is an illustrative example. The functions, figures and contingency wording are a composite drawn from anonymized Business Function Detail records at several banks. A bank adopting it should replace them with its own records and complete every item marked in red.

2. At a Glance

RTO is the time by which the function or resource must be running again. RPO is how much recent data could be lost. MTD is the longest outage the Bank can tolerate. All figures are in hours.

Function	Critical Level	Function RTO	Resource RTO	RTO Gap	RPO	MTD	Contingency Strategy
Fund loans and construction draws	Level 1	24 hrs	4 hrs	+20 hrs	24 hrs	48 hrs	Partially complete and hold
Prepare and submit the credit package	Level 1	24 hrs	4 hrs	+20 hrs	24 hrs	48 hrs	Partially complete and hold
Order third-party services (appraisals, inspections, flood determinations, title)	Level 1	48 hrs	4 hrs	+44 hrs	24 hrs	72 hrs	Use manual process
Borrower due diligence and document collection	Level 2	48 hrs	4 hrs	+44 hrs	24 hrs	72 hrs	Partially complete and hold
Collateral valuation review	Level 2	48 hrs	4 hrs	+44 hrs	24 hrs	72 hrs	Use manual process
Flood determination and insurance tracking	Level 2	48 hrs	4 hrs	+44 hrs	24 hrs	72 hrs	Partially complete and hold

The driving function, funding, must be running again within 24 hours. Against email's recorded 4-hour objective that is a cushion of 20 hours, but the cushion holds only if the provider actually restores service within 4 hours. A provider-wide outage can run past that point, and the Bank has no lever to shorten it, so plan the continuity procedure as though the cushion is not there.

Resource: App Environment Cloud-based (vendor-hosted software as a service); service provider Microsoft; recovery strategy Contact Vendor/Service provider. The 4-hour RTO is the figure most often recorded for email in the records behind this example, but it is the Bank's expectation, not a commitment from the provider, and the Bank cannot restore a hosted mail service itself. *[To be completed by the department: Time Frame Source and Time Frame Validation for the email RTO, for example the provider's service level terms or the Bank's own outage history]*

3. Activation

How the outage is recognized: Staff cannot send or receive mail in Outlook or Outlook on the web, messages sit in the outbox, or the provider's service health page reports an incident. *[To be completed by the department:*

whom staff report a suspected email outage to (help desk or IT on-call) and how, using a channel that does not depend on email]

Who declares the playbook in effect: the person named for that role in Section 6, after IT confirms the outage is not limited to one user or workstation.

Checkpoint	Elapsed Time	Action	Who (Section 6)
Detection	0 hrs	Confirm the outage with IT. Start the incident log. Notify the roles in Section 6 by phone or the Bank's approved alternate channel. Begin Section 5.	Incident lead
The resource's own recovery objective	4 hrs	Email's recorded objective has passed. Obtain a status update and estimated restoration time from IT. If none is available, assume the outage will continue past the funding deadline and contact today's closing agents and funding parties by phone.	Incident lead
Half the function RTO	12 hrs	Review every loan scheduled to fund or close in the next 24 hours. Confirm instructions and documents by the approved alternate channel, or reschedule with the borrower's agreement.	Loan officers and processors
Function RTO	24 hrs	Funding and credit package submission should be running again. If they are not, escalate to the person who declared the playbook and decide which closings to postpone.	Incident lead
Maximum tolerable downtime (MTD)	48 hrs	An outage beyond this point is unacceptable to the Bank for funding and credit package work. *[To be completed by the department: what the department does if email is still unavailable at 48 hours, for example an approved temporary mail service or secure file transfer for closing packages]*	Person who declared the playbook

4. First Hour

- Confirm with IT whether email alone is down or other Microsoft 365 services (Teams, SharePoint, OneDrive) are also affected. If Teams is down too, do not rely on it as the backup channel.
- Notify the roles in Section 6 by phone or the Bank's approved alternate channel.
- Start the incident log: time detected, who reported it, each status update, and each loan action taken outside email.
- Switch closing, funding and vendor correspondence to the department's back-channel mailbox, which is hosted on a different email provider (Section 5).
- Pull today's pipeline from the loan origination system: closings, fundings, draw requests, and third-party orders awaiting results.
- Begin the continuity procedure in Section 5, starting with the Level 1 functions.

5. Continuity Procedure

Fund loans and construction draws (Level 1)

Contingency Details recorded for this kind of function in the records behind this example:

> *"Partially complete and hold. Find another way to communicate if possible."*

Recorded description of a construction draw function:

> *"Need to order an inspection first"*

The recorded arrangements support these steps:

- Send closing and funding documents from the department's back-channel mailbox, which is hosted outside Microsoft 365 and already known to the Bank's settlement agents and title companies.
- Call each closing or settlement agent on today's list using the phone number already held in the loan file, not a number received in an email during the outage.
- Confirm wire instructions by callback before any disbursement. Do not accept changed instructions received through any channel during the outage.
- For construction draws, confirm the inspection is complete with the inspector by phone or through the inspection vendor's portal before releasing funds.
- Hold any funding that cannot be confirmed, and record it in the incident log.

[To be completed by the department: the back-channel mailbox address, its provider, and which closing agents, title companies and vendors have been given it]

Prepare and submit the credit package (Level 1)

Contingency Details recorded:

> *"Partially complete and hold. Find another way to communicate if possible."*

The recorded arrangements support these steps:

- Assemble credit packages in the loan origination system and on the network as usual.
- Route packages to Credit Administration through the loan origination system's workflow or a shared network folder instead of email.
- Tell approvers by phone that a package is waiting.

[To be completed by the department: who in Credit Administration receives packages during an email outage, and in which system or folder]

Order third-party services: appraisals, inspections, flood determinations, title (Level 1)

Contingency Details recorded for appraisal review at one bank in this example (vendor names removed):

> *"Email carries the vendor portals' notices that a completed report is ready. If email is unavailable, the appraisal department checks the vendor portals directly for completed reports and follows up with appraisers by phone."*

The recorded arrangements support these steps:

- Place new orders directly in each vendor's portal rather than by email.

- Check each portal at set times during the day for completed appraisals, inspections, flood determinations and title work, because the notices that normally say a report is ready will not arrive.
- Follow up with appraisers, inspectors and title companies by phone.
- Where a vendor cannot use its portal, ask it to send results to the department's back-channel mailbox.
- Record each order and each result received in the incident log.

[To be completed by the department: list of third-party vendors the department orders from, with their portal and support phone number]

Level 2 functions: borrower due diligence, collateral valuation review, flood determination and insurance tracking

Contingency Details recorded:

> *"Partially complete and hold. Use another means of communication if possible."*

The recorded arrangements support these steps:

- Continue work that does not need email, such as reviewing documents already received.
- Ask borrowers to upload documents through the Bank's secure portal or deliver them to a branch, rather than emailing them.
- Hold work that cannot continue, and note it in the incident log.

[To be completed by the department: the secure method borrowers use to send documents when email is unavailable]

6. Roles and Contacts

Role	Name	Responsibility
Incident lead (Commercial Loan Origination)	*[To be completed by the department: name of the incident lead and an alternate]*	Runs this playbook, keeps the incident log and reports status.
Declares the playbook in effect	*[To be completed by the department: name of the person who declares the playbook in effect and receives escalations]*	Decides the playbook applies, decides which closings to postpone, and receives escalations.
IT incident contact	*[To be completed by the department: IT on-call contact reachable without email]*	Confirms scope and relays status from the provider.
Back-channel mailbox monitor	*[To be completed by the department: who monitors the back-channel mailbox during an outage, and an alternate]*	Watches the back-channel mailbox, routes incoming documents, and logs what is sent and received.
Service provider	Microsoft, through the Bank's Microsoft 365 administrators	Restores the hosted mail service. The Bank's role is to open a support case and track the provider's incident.
Credit Administration contact	*[To be completed by the department: who receives credit packages during the outage]*	Receives and acts on credit packages.

Role	Name	Responsibility
Approves customer communication	*[To be completed by the department: who approves messages to borrowers and closing agents about delays]*	Approves what borrowers and agents are told.

7. Customer and Information Protection

Several of these functions are customer-facing: borrowers, closing agents, appraisers and title companies all expect email. Every function in this example carries a PII Disclosure Impact of Medium or High, because loan files hold tax returns, financial statements and account numbers.

The workarounds above move information to phones, vendor portals, shared folders and paper. Information Security should agree in advance which of these are acceptable, and staff should not forward loan documents to personal email accounts or text them from personal phones. *[To be completed by the department: Information Security's agreement on which alternate channels may carry borrower information]*

The back-channel mailbox carries borrower information outside the Bank's primary email system. *[To be completed by the department: Information Security's approval of the back-channel mailbox, including multifactor authentication and how its messages are retained under the Bank's record retention policy]*

An email outage is also an opening for fraud. Expect spoofed messages claiming to be from Microsoft, IT or a title company, and treat any request to change wire instructions during or just after the outage as suspect until confirmed by callback.

8. Restoration and Backlog

- Confirm with IT that mail is flowing both ways, inbound and outbound, before standing down.
- Expect a surge of delayed messages. Work the inbox in this order: closing and funding, credit approvals, third-party results, then everything else.
- Stop using the back-channel mailbox. Save every message sent or received there to the loan file, and tell counterparties to return to the primary addresses.
- Match each third-party result received through a portal against the order log, so nothing is ordered twice.
- Re-send any message whose delivery cannot be confirmed, and confirm with recipients that critical documents arrived.
- Confirm the function is back to normal: *[To be completed by the department: who confirms origination is back to normal and closes the incident]*
- Close the incident log.

9. After the Incident

- Record the incident: when email failed, when it was restored, and when origination was current again.
- Compare the actual outage against email's 4-hour RTO and against each function's RTO and MTD.
- Note what worked and what did not, and update the BIA records: contingency details, recovery notes and, where the outage showed them to be wrong, the email RTO.

- Test the back-channel mailbox at least once a year, including a message to and from a settlement agent, and confirm counterparties still have the address.
- Update this playbook, including the vendor contact list and the approved alternate channels.

10. Items to Complete Before Adoption

This draft carries 16 items for the department to complete before the playbook is adopted. Each is marked in red where it appears above.

Item	Section	Why It Is Needed
Time Frame Source and Time Frame Validation for the email RTO, for example the provider's service level terms or the Bank's own outage history	2. At a Glance	A 4-hour figure with no recorded source can make every gap in the At a Glance table look safer than it is.
Whom staff report a suspected email outage to (help desk or IT on-call) and how, using a channel that does not depend on email	3. Activation	Staff need one route for raising and confirming an outage, and the usual route may be email.
What the department does if email is still unavailable at 48 hours, for example an approved temporary mail service or secure file transfer for closing packages	3. Activation	The records say only to hold the work or find another way to communicate.
The back-channel mailbox address, its provider, and which closing agents, title companies and vendors have been given it	5. Continuity Procedure	Counterparties need to know the address before an outage, so that a new address appearing during one can be treated as suspect.
Who in Credit Administration receives packages during an email outage, and in which system or folder	5. Continuity Procedure	Without it, packages stall between the two departments.
List of third-party vendors the department orders from, with their portal and support phone number	5. Continuity Procedure	Staff cannot look up a vendor's contact details in an email they cannot open.
The secure method borrowers use to send documents when email is unavailable	5. Continuity Procedure	Borrowers may otherwise send tax returns and financial statements to personal or unmonitored accounts.
Name of the incident lead and an alternate	6. Roles and Contacts	Someone has to run the playbook and keep the incident log.
Name of the person who declares the playbook in effect and receives escalations	6. Roles and Contacts	Activation and the 24- and 48-hour escalations depend on it.
IT on-call contact reachable without email	6. Roles and Contacts	IT confirms the outage and relays the provider's status.
Who monitors the back-channel mailbox during an outage, and an alternate	6. Roles and Contacts	Messages sent to an unwatched mailbox are no better than messages that bounce.
Who receives credit packages during the outage	6. Roles and Contacts	Packages need a named recipient outside email.

Item	Section	Why It Is Needed
Who approves messages to borrowers and closing agents about delays	6. Roles and Contacts	Customer messages during an outage need one approver.
Information Security's agreement on which alternate channels may carry borrower information	7. Customer and Information Protection	Workarounds that move customer information outside managed systems need it.
Information Security's approval of the back-channel mailbox, including multifactor authentication and how its messages are retained under the Bank's record retention policy	7. Customer and Information Protection	A second mailbox on another provider needs the same protections and retention as the primary one.
Who confirms origination is back to normal and closes the incident	8. Restoration and Backlog	Stand-down needs a named decision.

11. Sources

- Composite of anonymized Business Function Detail records for lending departments at four BNP, Inc. client institutions, report dates May through November 2026. No client is named and no client-specific detail is used.
- Contingency wording is quoted from those records, with vendor names removed.
- Structure: BNP, Inc. Incident Response Playbook template, November 2026.
- This example is not any bank's adopted plan. Recovery figures are typical values from the records and must be replaced with the adopting bank's own.