

When Email Goes Dark
An Incident Response Playbook for the Narrow but Absolute Outage

Lessons from the November 2026 Microsoft 365 outage for community bank and credit union loan origination

---

Steve Carroll

Principal, BNP, Inc.

November 13, 2026

Table of Contents

Introduction..... 3

What happened on November 12..... 3

The narrow but absolute outage..... 4

What the BIA records show..... 4

Where email hides in commercial loan origination..... 5

Building the playbook..... 6

Decisions to make before the next outage..... 7

An example playbook..... 8

Conclusion..... 9

Sources..... 9

Introduction

The next interruption most banks and credit unions will face is probably not a hurricane, a flood, or a fire. It is more likely to be a narrow but absolute outage of a single service or vendor: one platform that the whole institution depends on stops working, while the building, the power, the network, and the people are all fine.

On November 12, 2026, that scenario played out for a large share of the industry at once. Microsoft's Exchange Online, the service behind Outlook email for most Microsoft 365 customers, began failing, and the disruption spread to other Microsoft 365 services. Nothing was wrong at any bank. Branches were open, cores were up, and staff were at their desks. They just could not send or receive email.

This article uses that outage to walk through how to build an incident response playbook for an email outage. It draws on anonymized Business Impact Analysis (BIA) records from BNP, Inc. client institutions to show how deeply email is woven into loan origination, using commercial loan origination as the worked example. It closes with an example playbook a bank or credit union can adapt. Where a point comes from published guidance or reporting, it is cited. Where it comes from BNP, Inc.'s own experience, it is labeled *Practice-based*.

What happened on November 12

The facts below are drawn from press coverage published while the incident was still open. Microsoft had not published a root cause at the time of writing, and some details may change when it does.

- **Two incidents, one platform.** Microsoft tracked the problem as Exchange Online incident EX1550543 and a broader Microsoft 365 incident, MO1550821, both listed as service degradations (SecurityWeek, November 12, 2026).
- **More than email.** SecurityWeek reported disruption to Exchange Online, Outlook, Teams, SharePoint Online, Microsoft 365 Copilot, and Defender XDR.
- **Not an attack, as far as was known.** SecurityWeek reported that affected servers "were failing automated health checks," that Microsoft was testing a workaround, and that there was no evidence of a cyberattack (SecurityWeek, November 12, 2026).
- **Into a second day.** Reports the following morning described the disruption continuing into November 13, with Microsoft reverting a recent network configuration change and saying its earlier actions "have not provided the anticipated relief" (WindowsForum, November 13, 2026).

For a BCM program, the duration is the important fact. A hosted email service was degraded for well over a working day. As the records below show, the recovery time objective (RTO) most institutions have written down for email is four to six hours.

The narrow but absolute outage

Practice-based. Traditional business continuity planning was built around the loss of a place: a branch flooded, an operations center without power, a data center that had to fail over. Those plans assume that if you can get people to a working location with working systems, the business can continue.

A software-as-a-service (SaaS) outage breaks that assumption. Relocating staff does not help, because the service is down everywhere. Failing over does not help, because the institution does not own the system and has nothing to fail over to. The outage is narrow, touching one service, but for the functions that depend on that service it is absolute.

This is not a niche risk. The Treasury Department's February 2023 report on cloud adoption cited an ABA estimate that SaaS adoption among banks was "around 91 percent" (U.S. Treasury, 2023). Email, document management, loan origination systems, vendor portals, and collaboration tools now run as somebody else's service. In BNP's DR testing article earlier this year, we traced how continuity testing has shifted from the institution's own data center to evidence obtained from those providers. The November 12 outage shows the other side of that shift: when the provider has a bad day, the institution's response depends on what it planned to do while it waits.

The FFIEC anticipates this. It warns that "An entity's third-party service provider can be a single point of failure" and that "A disruption in the delivery of those services can have a direct impact on entities' resilience" (FFIEC BCM Booklet, 2019, Section IV.A).

What the BIA records show

To see how much loan origination depends on email, BNP reviewed the current Business Function Detail reports for every lending and credit department at four client institutions: commercial, consumer, mortgage, SBA, and specialty lending, along with the loan processing, closing, funding, credit administration, and loan servicing groups that support them. The records were anonymized and counted in code. No client is named and no client-specific detail is used.

Finding	Count	What it means
Functions reviewed	231 functions in 33 departments	The full lending and credit footprint at four institutions
Functions that list email as a dependency	81 (35%), in 22 of the 33 departments	Email is a recorded dependency in two of every three lending departments
Email-dependent functions at Critical Level 1	24	Each must be running again within 24 hours
Recorded RTO for email	4 to 6 hours	Every record assumed a same-day recovery
Email dependencies with a specific workaround	4 of 81	The rest are blank (21) or generic (56)

Finding	Count	What it means
Functions that list Microsoft Office or Microsoft 365 but not email	27 more	On November 12, these failed at the same time

Two things stand out.

The workaround is usually not written down. The most common contingency detail for an email dependency, word for word, is "Partially complete and hold. Find another way to communicate if possible." Another 21 dependencies carry a strategy with no detail at all. That is a reasonable answer when the expected outage is four hours. It is not a plan for an outage that runs into the next business day, because "another way" has to be decided, approved, and tested before staff need it.

The recovery time is the institution's assumption, not the provider's commitment. A 4-hour RTO recorded against a hosted service makes every gap in the BIA look comfortable: a Level 1 function with a 24-hour RTO appears to have a 20-hour cushion. But the institution cannot restore Exchange Online. As we wrote in the DR testing article, recovery time frames for SaaS systems now need a source, and the FFIEC expects them to be "evaluated for alignment with third-party service providers' contracted recovery expectations" (FFIEC BCM Booklet, 2019, Section III.A). The records reviewed here did not cite one.

Where email hides in commercial loan origination

Practice-based. Commercial loan origination is a good test case because so much of the work depends on outside parties: appraisers, inspectors, flood determination vendors, title companies, attorneys, borrowers, and settlement agents. Each of those relationships runs on email, often without anyone thinking of email as a system. In BIA sessions, lenders and processors describe email not as a tool they use but as the place where work arrives.

Activity	How email is used	What breaks when it is down
Ordering appraisals	Engagement letters, vendor portal notices, appraiser questions	Orders placed in a portal still work, but the notice that a report is ready never arrives
Property and construction inspections	Scheduling, inspection reports, draw requests	Draws wait, because one record notes the bank needs "to order an inspection first"
Flood determinations	Determination certificates and life-of-loan notices delivered by email	Closings stall on a missing certificate, and insurance tracking falls behind
Title and closing	Title commitments, closing instructions, funding authorizations	Closing packages and funding confirmations cannot be sent, and the settlement agent is waiting

Activity	How email is used	What breaks when it is down
Credit package and approval	Packages routed to credit administration, approvals returned	Approvals wait even when the loan system is up
Borrower documents	Tax returns, financial statements, and borrowing base reports	Borrowers keep sending to an inbox no one can open, or try personal accounts

The appraisal row illustrates the most common hidden dependency. At one institution, appraisal reports are retrieved from vendor portals, but email carries the portal's notice that a report is ready. That institution did write the workaround down: "If email is unavailable, the appraisal department checks the vendor portals directly for completed reports and follows up with appraisers by phone." That single sentence is what turns a generic contingency into a usable one. It names the alternate channel, the task, and who does it.

Building the playbook

An incident response playbook is a short operational document that tells a department what to do from the first sign of an outage until the backlog is cleared. It is narrower than a business continuity plan. It covers one resource, here email, and every function that depends on it, in priority order. The FFIEC expects "event management procedures that detail reasonably foreseeable event types" and says procedures "should be clear, concise, and easy to implement in an emergency" (FFIEC BCM Booklet, 2019, Sections V.A and V.B). An email outage is now a reasonably foreseeable event.

BNP builds these playbooks directly from the BIA records, so the figures and recorded workarounds in the playbook match what the department said in its BIA. Where the records are silent, the playbook says so instead of filling in a plausible answer. The structure is the same for any resource:

1. **At a glance.** List every function that depends on email with its Critical Level, its RTO, email's RTO, the gap between them, and the maximum tolerable downtime (MTD). Order them by criticality, then by the tightest gap.
2. **Activation.** Say how staff recognize the outage, whom they report it to without using email, and who declares the playbook in effect.
3. **Escalation checkpoints.** Tie actions to elapsed time: detection, email's own recovery objective, half of the driving function's RTO, the function RTO, and the MTD. At each checkpoint, name the action and the role.
4. **First hour.** Confirm scope with IT, notify the roles by phone or another approved channel, start an incident log, and pull today's pipeline of closings, fundings, and third-party orders.
5. **Continuity procedure.** For each function, quote the recorded contingency detail, then list the steps it supports. Where the record says only "find another way," that is an item for the department to complete before adoption.

6. **Roles and contacts.** Name the incident lead, the person who declares, an IT contact reachable without email, and who approves messages to customers. Keep vendor contact numbers somewhere other than an inbox.
7. **Customer and information protection.** Decide in advance which alternate channels may carry borrower information, and plan for the fraud that follows outages.
8. **Restoration and after-action.** Work the backlog in priority order, confirm nothing was lost or sent twice, and update the BIA with what the outage actually showed.

Decisions to make before the next outage

Practice-based. Most of the hard parts of an email playbook are decisions, not procedures. They are easier to make on a quiet afternoon than at 2:00 p.m. on a closing day.

- **What is the approved alternate channel?** The FFIEC expects management to "plan for, and prepare multiple mechanisms to communicate with others" (FFIEC BCM Booklet, 2019, Section IV.B). On November 12, Teams was affected too, so a plan that falls back from Outlook to Teams falls back to the same platform. Consider the phone, the loan origination system's own messaging, vendor portals, and a secure file transfer or borrower portal that sits outside Microsoft 365.
- **Should the department have a back-channel email address?** *Practice-based.* One practical answer is a pre-arranged "back channel": a department mailbox hosted on a different email provider, outside Microsoft 365, that is used only when the primary service is down. For commercial loan origination, it lets closing packages, funding confirmations, and third-party results keep moving by email when Outlook cannot. It only works if it is set up before it is needed. Give the address to settlement agents, title companies, appraisal and flood vendors in advance, so they recognize it and so a new address that first appears in the middle of an outage can be treated as suspect. Have Information Security approve it, turn on multifactor authentication, and confirm messages are retained under the institution's record retention policy. Assign who monitors it, and test it during the year, not on the day of the outage.
- **Where do contact lists live?** If the appraiser, inspector, title company, and settlement agent phone numbers exist only in old emails, staff cannot reach them. Keep a current vendor contact list in the loan origination system or on paper.
- **What happens to customer information?** Most lending functions in the records reviewed carry a Medium or High PII Disclosure Impact. Workarounds that move tax returns and financial statements to personal email, text messages, or USB drives need Information Security's agreement in advance, or a clear "do not."
- **What is the fraud rule?** Email outages are followed by spoofed messages claiming to come from Microsoft, IT, or a title company. Make it a standing rule that wire instructions received or changed during or just after an outage are confirmed by callback to a number already on file.
- **What is the real RTO?** Replace the assumed 4-hour figure with a sourced one: the provider's service terms, its published incident history, or the institution's own experience, including

November 12. If the honest figure is longer than a Level 1 function can tolerate, that is the gap the playbook exists to close.

An example playbook

The example playbook that accompanies this article covers Commercial Loan Origination during a full email outage of up to 48 hours. It was generated with BNP's incident response playbook tooling from a composite of the anonymized records described above. Its priority order is:

Function	Critical Level and RTO	Recorded contingency
Fund loans and construction draws	Level 1, 24 hours	Partially complete and hold
Prepare and submit the credit package	Level 1, 24 hours	Partially complete and hold
Order third-party services (appraisals, inspections, flood, title)	Level 1, 48 hours	Use manual process
Borrower due diligence and document collection	Level 2, 48 hours	Partially complete and hold
Collateral valuation review	Level 2, 48 hours	Use manual process
Flood determination and insurance tracking	Level 2, 48 hours	Partially complete and hold

Its escalation checkpoints fall at detection, 4 hours (email's recorded objective), 12 hours (half the funding RTO), 24 hours (the funding RTO), and 48 hours (the funding MTD). The continuity steps come from what the records say: switch closing and vendor correspondence to the department's back-channel email address, call settlement agents on numbers already in the loan file, confirm wire instructions by callback, place third-party orders and check results directly in vendor portals, route credit packages through the loan system instead of email, and ask borrowers to use a secure portal.

The example also carries 16 items marked for the department to complete before adoption, such as the name of the incident lead, the back-channel mailbox and who monitors it, the vendor contact list, and Information Security's agreement on alternate channels. Those blanks are deliberate. A playbook that reads complete but carries an invented step or phone number is worse than one with an honest blank, because staff will follow it during an outage.

Conclusion

The November 12 Microsoft 365 outage did not damage a single branch or server at any bank. It still stopped closings, appraisal follow-ups, credit approvals, and borrower document collection at institutions that had written down a 4-hour recovery time for email and "find another way to communicate" as the plan. That is the shape of the modern interruption: narrow, absolute, and outside the institution's control.

The fix is not a new disaster recovery site. It is a short playbook for each critical SaaS dependency, built from the BIA, that names the alternate channel, such as a back-channel mailbox on a different provider, the people, the checkpoints, and the information protection rules before they are needed. Email is a good place to start, because every department depends on it, and because most institutions have just watched what happens without one.

Sources

1. Federal Financial Institutions Examination Council, FFIEC IT Examination Handbook: Business Continuity Management, November 2019, Sections III.A, IV.A, IV.B, V.A, and V.B.
2. SecurityWeek, Microsoft 365 Outage Disrupts Outlook, Exchange Online and Teams, November 12, 2026.
3. WindowsForum, Microsoft 365 Outage Investigation: Secure Connection Overload and Network Rollback, November 13, 2026.
4. U.S. Department of the Treasury, The Financial Services Sector's Adoption of Cloud Services, February 2023.
5. BNP, Inc., anonymized Business Function Detail reports for 33 lending and credit departments at four client institutions, report dates May through November 2026.

Statements marked *Practice-based* reflect BNP, Inc.'s experience supporting banks and credit unions and are not drawn from the sources above.