Welcome!

BPM (Business Processing Manager) is an application designed and developed for managing multi-tiered complex workflow processes. While this document is your initial guidance to deploy and implement BPM it also serves as an on-line help library.

BPM supports Apple IOS, Android, and Windows devices. BPM is more than an incident workflow application but also as multi-tiered complex workflow that provides coordination of multiple teams executing a single plan with multi-tasks or work streams made up of multiple task streams. BPM can also support a hierarchy of complex multiple workflows bonded together.

BPM can support healthcare emergency procedures, disaster recovery, cyber events, police and fire search and rescue (via drones), and military applications. Additional license entablements may be required for certain advanced features.

You can use BPM with up to 5 users at no charge, supporting one complex workflow plan, with one sequence, and 25 tasks, more complex configurations will require a low monthly fee shown in the pricing section at https://www.acomdev.com/pricing .

Tasks are dispatched to users via their email address and as a text, automated backup teams may be engaged as needed. Real-time dashboards show workflow executions with advanced graphics.

Please follow the on-boarding document and at any time do not hesitate to reach out to support@acomdev.com and/or to me personally if you are having difficulty. I want this to be a positive experience for you; we are only as far away as a phone call or email.

Thank you for trying BPM, I truly hope you find it helpful, and if you see an area for improvement or have any suggestions, we would love to hear from you.

Thank you,

Table of Contents

BPM Versions

Modules	Version	Downloadable	
BPM Windows Control	1.1.5	https://www.acombpm.com	
BPM Apple IOS	1.1.4	Apple Store	
BPM Android	1.1.2	Google Play Store	

Certifications

CMMC	Security Level One	6/1/2025	
CMMC	Security Level Two	In-process	
Enterprise Readiness Overview	ACOMdev Security Statement	Appendix A	

A little history about BPM (and a lesson learned)

I've worked in IT for more than 30 years, starting as an engineer and developer, moving into management, then advancing to Director, CTO, and ultimately CIO for two automotive manufacturing firms, both domestic and international. Over that time, I've worked in data centers around the world and seen the same pattern repeat.

Teams that are highly organized in day-to-day operations can become confused and fragmented during a true emergency, especially when the situation requires specialized skills and a complex sequence of steps to restore service. That's one of the reasons disaster recovery planning exists, not because people don't know what to do, but because executing under pressure is fundamentally different than operating under normal conditions.

A Personal Experience

While serving as Senior Director for an automotive company based in Columbus, Indiana, we operated a primary data center in Indianapolis (about 30 miles north). It was a professional, well-run facility, well known in the area and shared by several major Midwest corporations. It housed racks of our ERP and database servers supporting a global manufacturing operation: 33 sites worldwide and roughly 8,000 employees.

At the time, I was responsible for two data centers:

- **Indianapolis, Indiana**
- **Augsburg, Germany**

We also ran two ERP platforms:

- **QAD MFG/Pro**, hosted in Indianapolis, supporting all manufacturing sites across the Americas and a couple of locations in China.
- **SAP**, hosted in Augsburg, and supported European operations.

The two environments were linked, and we mirrored data across the Atlantic using what was new technology at the time: **Data Domain**. What impressed me most about Data Domain was how efficiently it managed ongoing backups. The first full backup took longer because it created a complete encrypted and compressed copy. But after that, the system backed up only changed data blocks. Within a month, backups that used to take hours were completed in minutes. It worked extremely well, and we deployed it in both Indianapolis and Augsburg.

The Outage

One morning in mid-2008, August, if I recall correctly, I was driving to the office when calls started coming in from across the U.S., users couldn't log into our ERP system.

In automotive manufacturing, an ERP outage is a major business event. You're not only losing production and revenue, but contract obligations may also impose penalties if delays begin impacting a customer's production line.

A few quick calls to my team confirmed the situation: it appeared **all systems were offline**. They had already contacted the data center and were told there had been a major power failure. The entire building was down.

Why This Hit Hard: A Lesson from Germany

A colleague of mine experienced a serious outage in Germany about six months prior, two hard drives failed in a storage array supporting a plant supplying a leading German automaker. The drive failure happened over the weekend. Normally that shouldn't take an array down, but the environment wasn't being properly monitored, and a second drive had already failed weeks before without anyone aware. When this next failure occurred, the array collapsed, the database went down, and the ERP system went with it.

There's an important lesson to be learned, the array was about six years old, meaning all the disk drivers were also six years old. When one drive fails due to age, the odds are others will fail increasing the risk. That's why monitoring and proactive maintenance is extremely important. I cannot stress the importance of properly monitoring systems.

Recovery took about six hours, sourcing drives, installing and formatting them, rebuilding the array, reinstalling the database, and bringing ERP back online. Customer operations were impacted for almost three hours. The penalty at that time was **$1,000 per minute** (I'm sure it is higher now):

- 3 hours × 60 minutes = 180 minutes
- 180 × $1,000 = **$180,000**

Two drives that cost roughly $500 each, about $1,000 in hardware, drives in an array that could have been replaced without an outage since arrays will recreate lost date for a replacement drive using parity data, but not when two drives fail. Had proper monitoring been in place, when the first drive failed several weeks before the drive failure that took the system down, it could have been replaced over the weekend without causing a system outage.

This resulted in $180K in penalties, not to mention the damage to customer confidence.

Back to August 2008, when I heard “everything is down” in Indianapolis, I immediately understood the potential scale. And this time, the impact wouldn’t be limited to one plant, it could ripple across multiple facilities.

Walking Into the Facility

My team was already in route. I arrived about 15 minutes behind them, fielding call after call from increasingly frantic plant managers. When I reached the facility, someone had to manually let me in because automated door locks weren’t working, never a good sign.

Inside, it was a madhouse. Multiple companies were converging in the same building, all dealing with major outages at once. Partial power began to return, and we were finally able to assess the damage.

The root cause turned out to be a utility-related event, work on nearby power lines triggered **two surges**, followed by a **total power failure**. As systems began powering up, we found damaged power supplies and failed hard drives.

The utility and building operations confirmed the issue had been corrected, but recovery still required parts replacement, installation, validation, and testing before we could safely bring services back online. Fortunately, we had spare power supplies and drives, which helped us recover faster.

Where BPM Entered the Picture

If you’ve never been inside a data center, it’s difficult to appreciate how constrained the environment can be. Floors are segmented, isolating one company’s servers from another and are packed tightly together, with cages used for physical security that restrict access, which is good for security but challenging during emergency repairs.

We had several engineers literally working on top of one another: replacing power supplies, repairing a switch, swapping failed drives in a database array, all in close proximity. My team was steady and methodical making progress, and most systems were coming back online.

Across the way, another company’s situation looked much worse. We had installed dedicated UPS-protected power in each rack that filtered much of the surge. Our neighbors didn’t have that redundancy, and the damage to their equipment was far more severe. When their manager arrived, things deteriorated quickly: lack of direction or coordination, dropped tools, a cart with spare parts was knocked over, people frantically rushing and pressure escalating instead of stabilizing.

Watching that unfold, something clicked for me.

They didn't just need a solid recovery plan.

They needed a **coordinated execution plan**.

A plan can be well-written, and the people can be highly skilled, but under stress the wrong people get pulled in at the wrong time, work becomes chaotic, priorities blur, and recovery slows down. In that moment, I realized what was missing wasn't knowledge, it was **orchestration**.

That's where BPM comes in.

BPM as Disciplined Execution Under Pressure

In a disaster recovery event, tasks must happen in the right sequence, with the right roles, and with clear handoffs. For example, when you're replacing power supplies and failed drives, you do **not** need:

- the DBA
- software developers
- or managers in the middle of the work area

BPM, at its core, helps ensure:

- The right people are engaged at the right time.
- The work follows an orderly sequence.
- handoffs are explicit and controlled.
- progress is visible and verifiable.
- disruption from unnecessary involvement is minimized.

In other words: BPM "dispatches" the right skills to the right task at the right time, guided by a defined, repeatable execution plan.

A Simplified Example Flow

Here's a simplified example of what that coordination looks like:

1. **Facility management** verifies stable power and environmental conditions.
2. **Hardware technician** replaces failed components, powers up, and confirms basic operation.
3. **System administrator** restores system services and recovers lost data.
4. **DBA** validates database integrity and confirms readiness.
5. **ERP administrator** verifies application functionality end-to-end.
6. **Manager** communicates service restoration and authorizes user access.

These people don't just have specific tasks to accomplish, they need to be dispatched as needed, but not all at once.

The Takeaway

Disasters are high-pressure events. But with:

- a solid plan
- well-trained people
- clearly defined roles and responsibilities
- and tasks dispatched in a controlled, coordinated sequence.

…you can turn a chaotic recovery into a disciplined execution.

That experience is where BPM became real for me, not as theory, but as a practical method for coordinating complex work when the stakes are highest.

BPM Workflow

BPM supports the creation of a complete disaster recovery plans and emergency management strategies, from initial planning through testing, certification, and promotion to executable status.

BPM's origin: built from real-world disaster experience

BPM evolved from firsthand experience managing a real-life IT disaster. The team I led at that time was, without question, the strongest overall team I have had the privilege to work with in my 30-year IT career since leaving the Marine Corps in 1972.

That team executed a $3B carve-out of global IT infrastructure in less than nine months. We transitioned from being part of Fortune 500 to becoming a separate, private equity–owned global automotive manufacturing company, 33 sites and more than 8,000 employees world-wide. Separating email and user accounts, ERP platforms, and global quality systems is not a minor task. Senior leadership selected me to lead the IT carve-out, and I was trusted to hand-pick the team, systems, and infrastructure required to complete it.

The moment it became a disaster—and the lesson it created

During that nine-month period, my team and I not only delivered the carve-out, but we also developed a comprehensive disaster recovery plan. There wasn't a project too complex or difficult for this team to solve. Even on the day our data center lost power, and we faced a full-blown outage, the team responded professionally and efficiently. We restored operations and were back online within four hours.

That event also gave me a broader perspective. As we recovered, I watched neighboring companies, sharing the same data center, struggle with worsening conditions. It was an education to see how quickly panic and confusion can derail recovery efforts. In several cases, the damage to those organizations appeared severe enough to threaten their ability to continue operating.

The reality is simple: many businesses, especially small and mid-sized organizations, do not survive major disruptions. This is exactly why disaster recovery and business continuity planning must be structured, tested, documented, and kept current, not treated as a one-time exercise.

Enter BPM: a structured system to build, test, and maintain "ready-to-run" plans

BPM is designed to help organizations build robust, well-documented disaster recovery and business continuity plans, and to manage the entire lifecycle of those plans through real testing. The goal is not to create a binder on a shelf, but a plan that is complete, verified, and executable.

Key BPM capabilities include:

- **Guided plan development** that ensures critical components are captured and documented
- **Live testing (rehearsals)** to validate the plan end-to-end and expose gaps
- **Repeatable re-testing** to improve execution time and efficiency with each rehearsal
- **Dashboards and tracking** that document progress, steps completed, and readiness status
- **Promotion to executable status** once testing meets defined acceptance criteria

Operational resilience features built for real incidents.

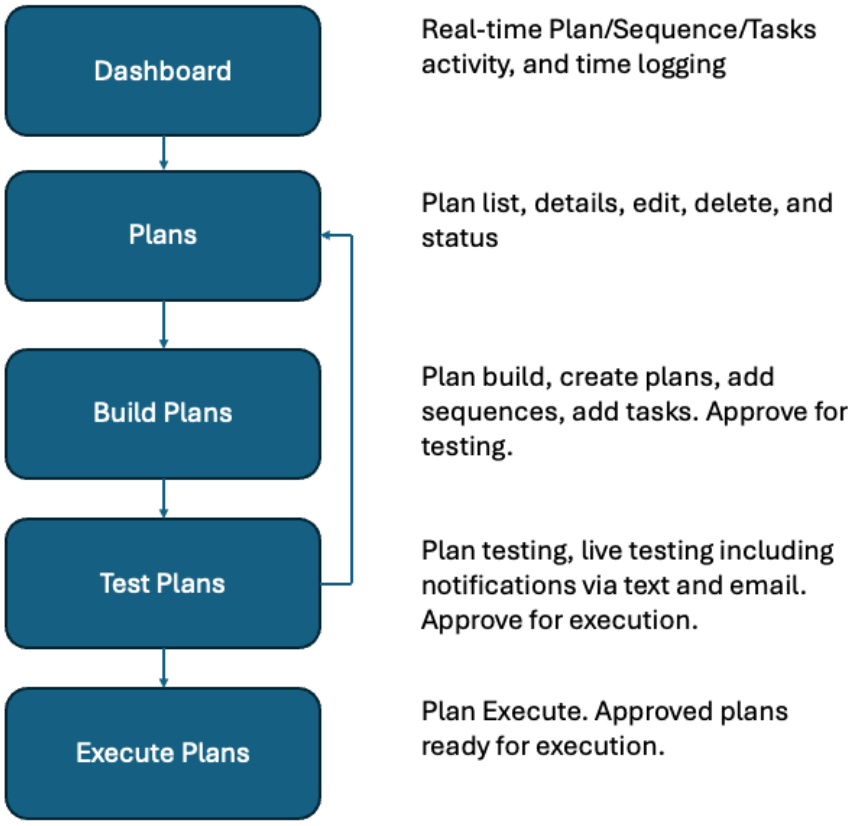
BPM also includes operational controls that set the standard during emergencies:

- **Annual reminders** to re-test and re-certify plans
- **Role and responsibility tracking**, including primary and backup personnel
- **Automated backup engagement**, if a key person is unavailable, BPM escalates to the designated backup
- **Administrative functions** to manage users, permissions, and plan support data

To support practical use in the field, BPM supports **iOS and Android mobile devices**, with a **Windows master console** for centralized management.

What follows:

Below is a high-level flow chart showing the steps BPM uses to build, test, certify, and promote a plan to executable status. Also included is a dashboard view for real-time status and updates.



(The administrative functions, user management, permissions, and supporting reference data are documented at the end of this document.)

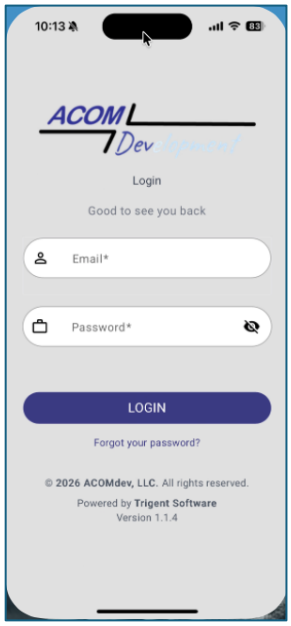
BPM On-boarding Process

Apple users, go to Apple App Store, search for ACOMdev BPM, then download the application.

Android users, go to Google Play on your Android and search for ACOMdev BPM and download it.

Windows users, BPM is compatible with most Windows based operating systems: Windows 10 and Windows 11, and most server operating systems. Click this link to access the Windows version of BPM. https://www.acombpm.com

After you've downloaded the application from Apple or Google the operation of BPM will be the same. When ACOMdev first starts you will see the screen below, note the Setup button circled in red. Click this first to create your administrative account. You will need your user email address and a “strong” password that you choose.



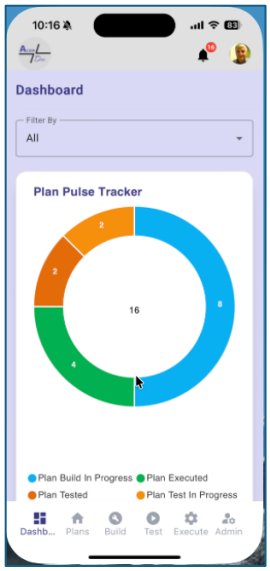
Setup

Upon clicking the Setup button, BPM will ask you for your e-mail address and desired password. The password should be a complex password made up of letters, numbers, and special characters; the minimum requirement is 16 characters.

When creating (or resetting) an account password you will be required to accept our user policy and authorization for text messaging.

First time logging in

After you have logged in, the first step is to go to the admin (administrator) menu and create users, following user creation create other key system categories such as sites, departments, skills, etc.



View Workflows/Plan

Workflows and certain functionality can be viewed from any device but may be limited based on user profiles and/or credentials. The below plans are displayed using both the Desktop and Mobile application displays. The desktop view and mobile view are not required to execute together; both can operate independent of each other.

Each “Workflow Plan” displays the name and creation date along with various status messages:

- Plan Build in Progress
- Plan Ready to be Tested
- Plan Test in Process
- Plan Tested
- Plan Executed

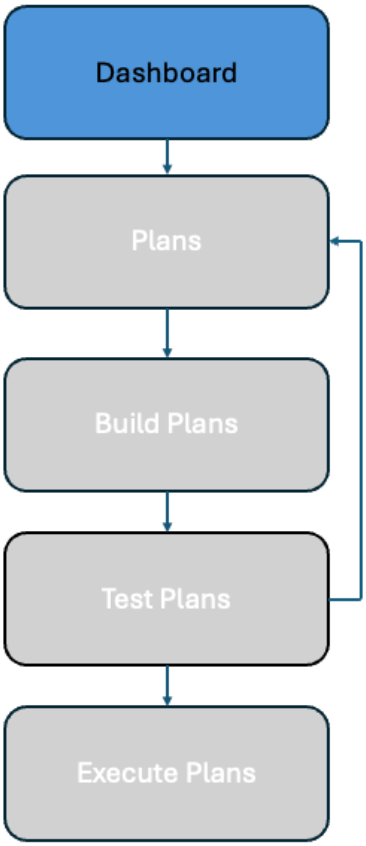
Basic navigation for this document screen examples.

In the examples shown throughout this document we will show both the desktop view on the left side (Windows application), and the mobile view on the right side (mobile application - mostly Apple iOS), please note Android displays are almost identical to the Apple version, to avoid cluttering the pages only the Apple view is displayed.

As you can see on the desktop view in the left most menu (black background) the menu items selected in this example is “Plans” circled in yellow. Correspondingly on the right, the mobile view, the menu item select at the bottom of the mobile screen is also “Plans” and also highlighted with yellow.

BPM supports disaster recovery, business continuity, emergency planning, cyber incident, general business operations, healthcare, police, fire, and military plans.

Dashboard



Dashboards

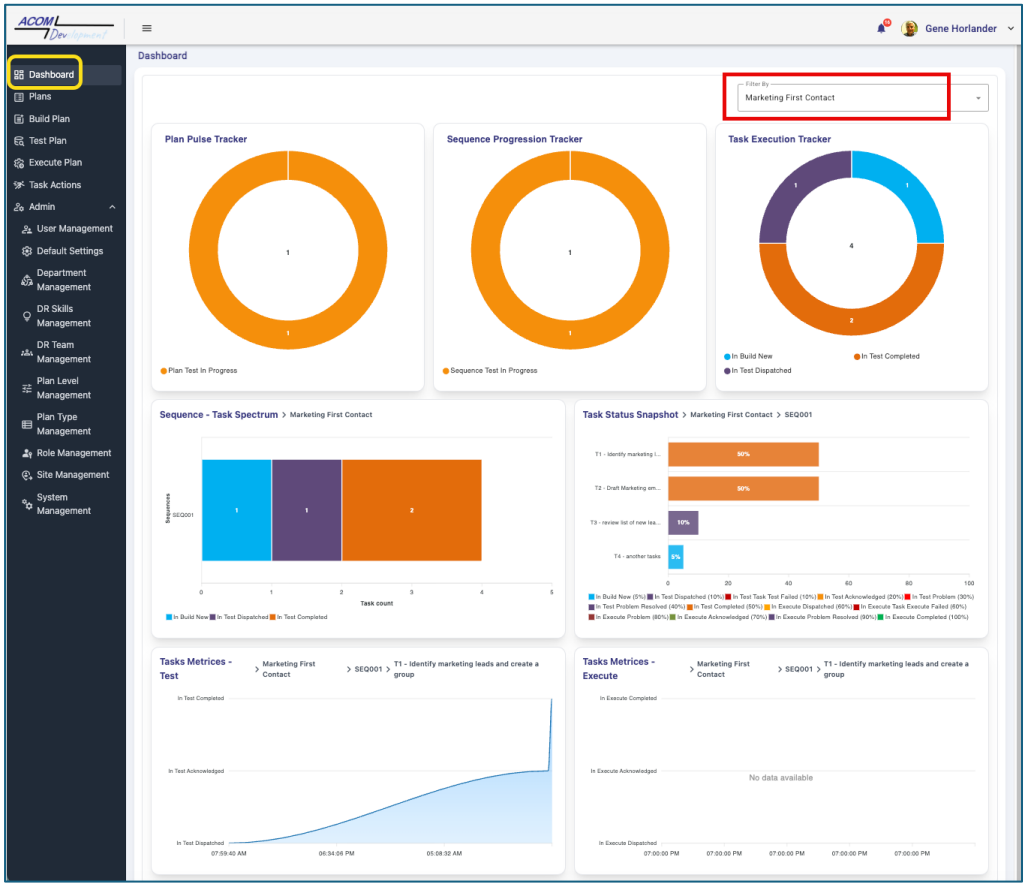
All dashboards within BPM are real-time, and all data is updated immediately. Dashboards are included in all three platforms for BPM: Windows, Apple IOS, and Android, and functional identically. Our licensing entitles you to all three versions of the application.

BPM dashboards provide workflow real-time status and execution times. Dashboard data is archived in BPM historical files and can be exported to Power BI for analytical reporting. Several Power BI reports are included with BPM, and all have drill down capability.

Sample reports:

- Workflows/Plans, default all, but can be filtered by plan
- Sequence/Task overview by workflow, and by workflow/plan

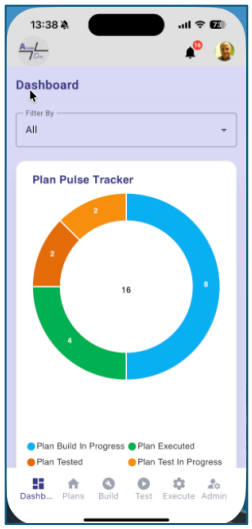
Dashboard Desktop View:



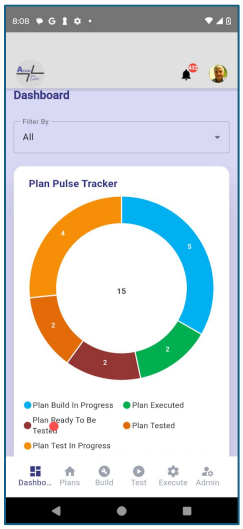
Upon login to BPM on an Apple IOS or Android device the first screen is always the dashboard. Across the bottom of all mobile device screens are command shortcut buttons. From left to right are: **Dashboard, Plans, Build, Test, Execute, and Admin**.

All functions within BPM are provided regardless of platiform used: Windows, IOS, or Android.

Apple IOS Version

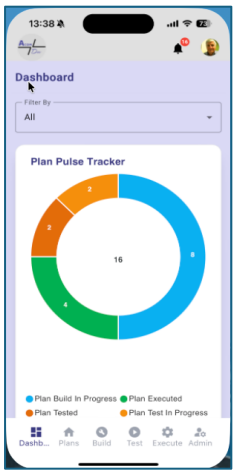


Android Version

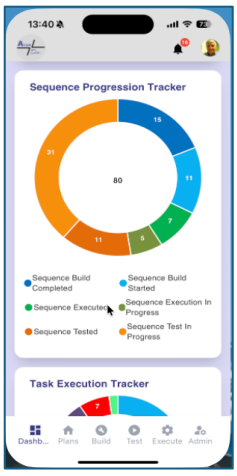


The dashboard provides graphical representation of several areas in BPM. The number of **Workflows** in BPM, **Sequences** per workflow (by plan), and number of **Tasks** (by sequence). Included is a breakdown by Task Spectrum, this can be filtered by plan id.

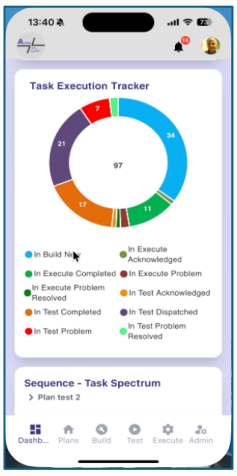
Plan Pulse Tracker



Sequence Tracker

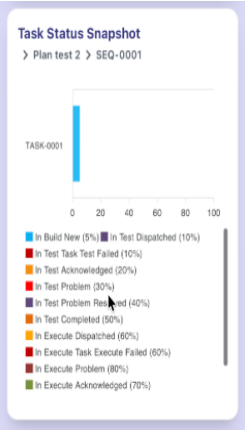


Task Execution Tracker



Sequences in a Plan

Task Status Snapshot



Task Execution

Plan Categories

- Plan Build in Process
- Plan Ready to be Tested
- Plan Test in Progress
- Plan Tested
- Plan Executed

Sequence Tracker

- Sequence Build Started
- Sequence Build in Progress
- Sequence Test in Progress
- Sequence Tested
- Sequence Execution in Progress
- Sequence Executed

Task Execution Tracker

- In Build – New
- In Test – Dispatched
- In Test - Acknowledged
- In Test – Problem
- In Test – Problem Resolved
- In Test – Completed
- In Execution – Dispatched
- In Execution – Problem
- In Execution – Problem Resolved
- In Execution - Completed

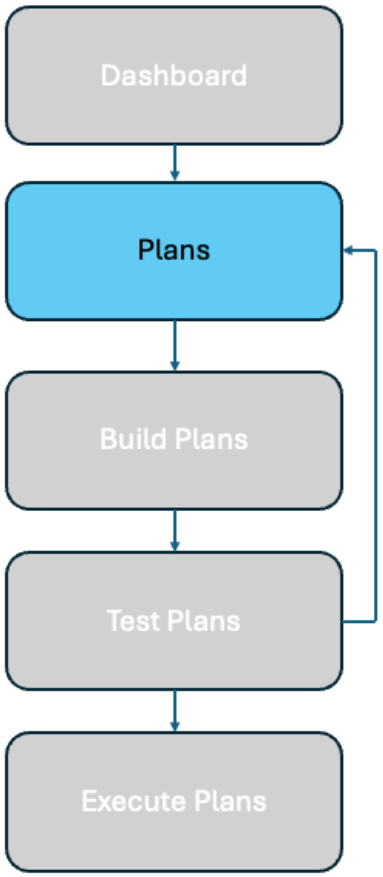
Dashboard Details:

The BPM dashboard is a very powerful and flexible monitoring solution for all Workflows including multiple sequences and tasks. The dashboard can track multiple plan executions within complex workflows and their combinations of workflows bonded together for advanced solution and functionality monitoring. The dashboard is highly configurable and can be easily customized to adapt to any workflow monitoring requirement.

One powerful feature of BPM dashboards is the ability to track in real-time plan execution. Thus allowing performance to be measured and reviewed; while repeatedly testing “rehearsing” complex workflow to improve the execution, quality, and to identify missing steps or areas where the plan can be improved.

All phases of a task are measured in each plan, sequence, and tasks from dispatching of the task to acceptance and completion. This process helps teams fine tune and improve the workflow. All test executions are also logged to the archive history files.

View a Plan

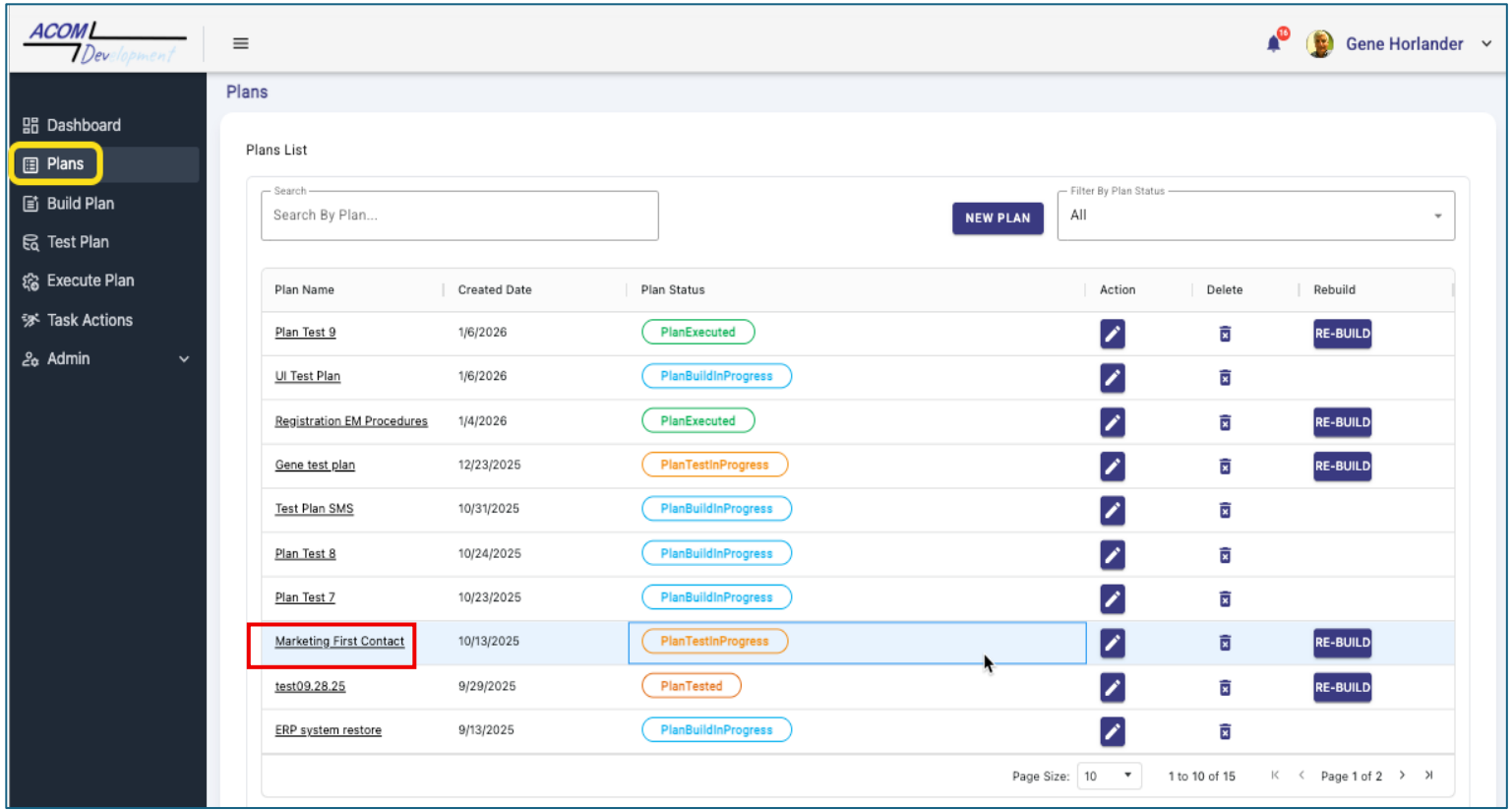


A list of active plans in various stages of completion are displayed on the desktop and mobile views of BPM "Plan" menu: Plan Name, Creation Date, Plan Status, along with Action/Delete/Rebuild options.

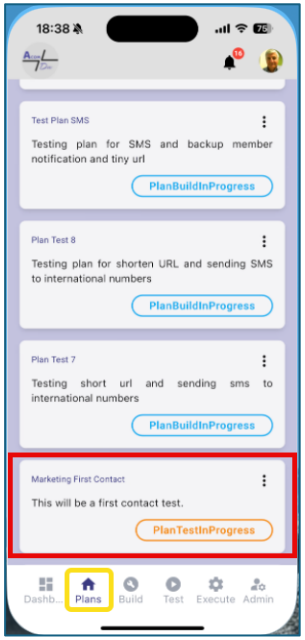
In the following example, we will view a plan called "*Marketing First Contact*," which is highlighted in red on both views. Please note the status is "**PlanTestInProgress**."

Plan: *Marketing First Contact*

Desktop View



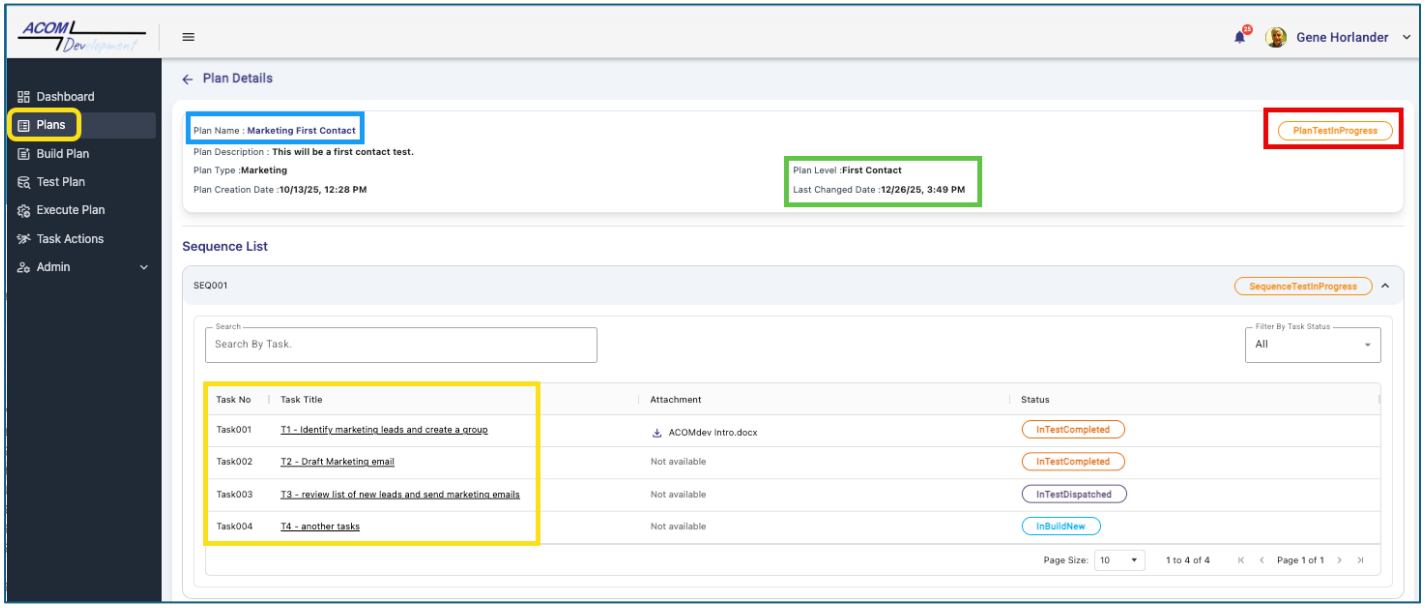
Mobile View



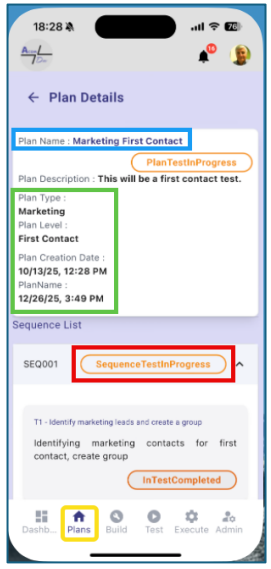
The left view is the desktop view of BPM, and on the right the mobile view(s). Desktop views use a horizontal landscape, and Mobile views Vertical. With mobile views, at times depending on the application in order to show the entire mobile screen there may be two mobile views, this is due to mobile device formatting. The plan name is displayed in both the desktop and mobile views, highlighted with a blue outline – Marketing First Contact. The area marked with red shows the plan's current status, in this case "**PlanTestInProcess**." Green outline show assigned users and activity dates, yellow the tasks list.

Plan: *Marketing First Contact*

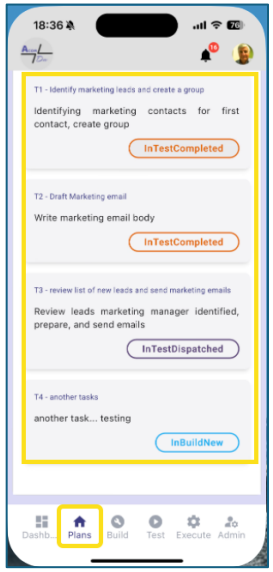
Desktop View



Mobile View #1



Mobile View #2



Highlighted in yellow, the" Marketing First Contact" plan had one sequence named "SEQ001" and embedded within SEQ001 are four tasks: T1, T2, T3, and T4. BPM plans can manage multiple threads of tasks activity. Tasks that can operate in parallel are maintained in a separate sequence, i.e. SEQ001, SEQ002…

For example, if a workflow is managing the construction of a building, while carpenters are doing finish work inside the new building, managed by Sequence #1, brick masons could be laying brick on the exterior of the building, this could be Sequence #2, and so on.

In the *Marketing First Contact* example, only one sequence was needed which is SEQ001. Within SEQ001 are four tasks, listed below. In this "snapshot" view, the first two tasks are complete, and third is dispatched via text and email, and the fourth tasks waiting to execute.

As tasks execution status is tracked and catalogued, along with execution times: how long did it take to dispatch the task, when did the team member accept it, and when was it completed?

Note that task T1 has an attachment, each task description field allows for 500 characters, attachments are used when more detail information is needed for a given task. Documents supported: Word, PDFs, spreadsheets, videos, photos, etc.

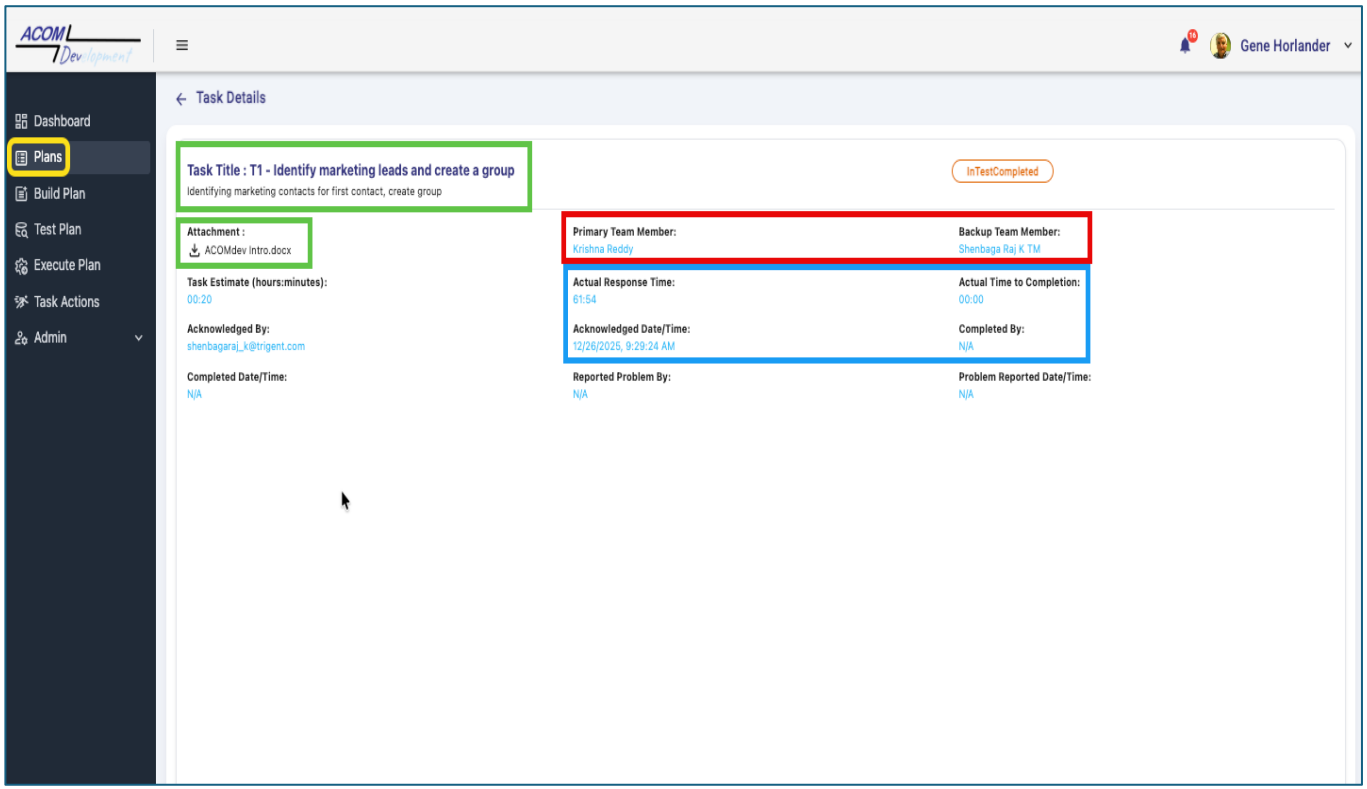
Plan: *Marketing First Contact*		
Tasks	Status	Attachment
T1	**InTestCompleted**	Yes
T2	**InTestCompleted**	
T3	**InTestDispatched**	Means task sent via email and text to team member
T4	**InBuildNew**	Waiting to execute

Workflow Details

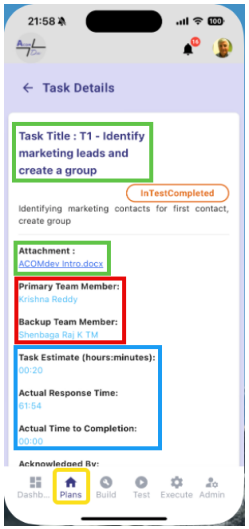
By drilling down on a given task, we can see more details. Highlighted in green is the task name. a short description. Red highlights the primary and backup team members. Every task in all plans requires a primary team member and backup. Highlighted in blue are time loggings of task activity. The data and time of when the task was dispatched and when the team member accepted the task is logged and displayed on the dashboard.

Plan: *Marketing First Contact*

Desktop View



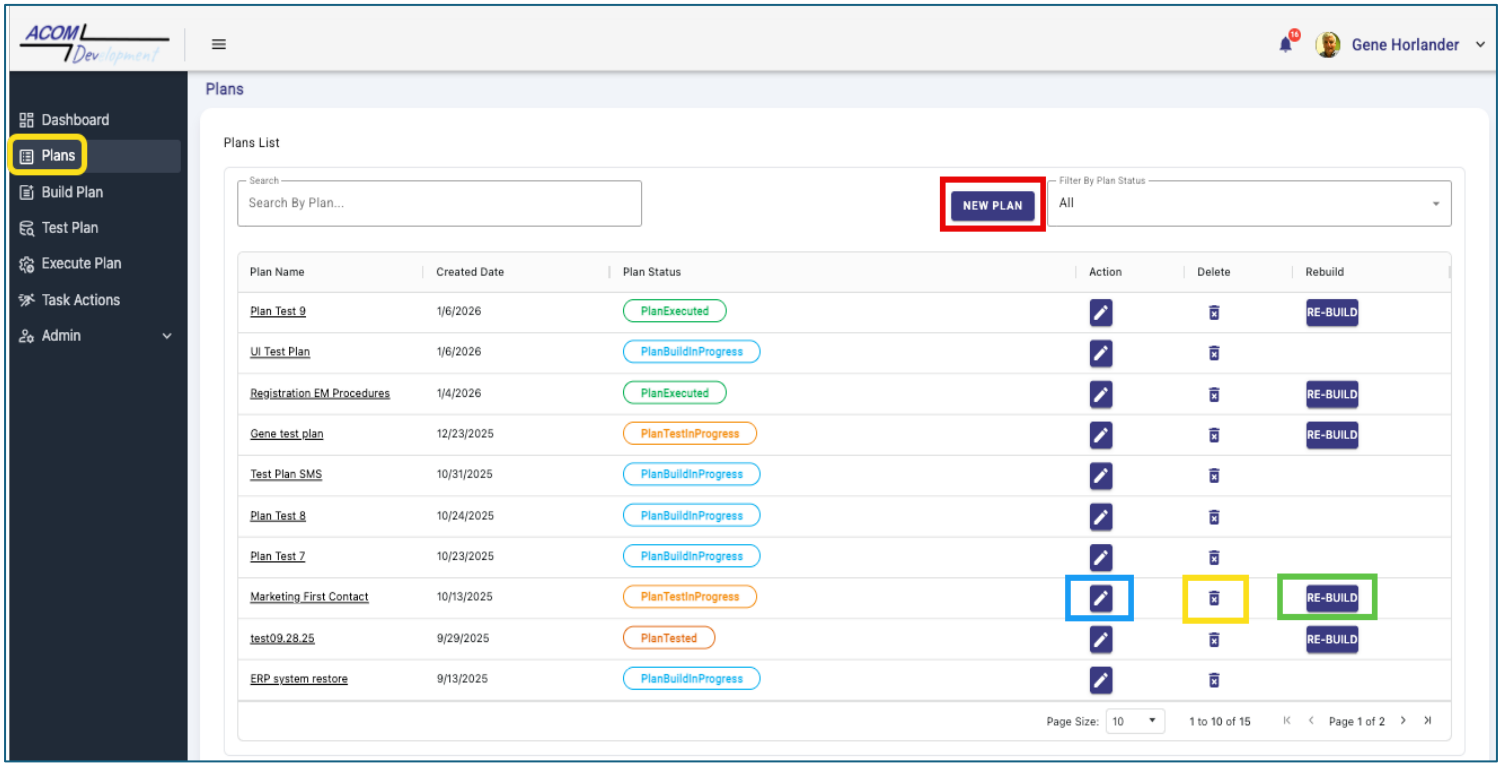
Mobile View



Workflow Options

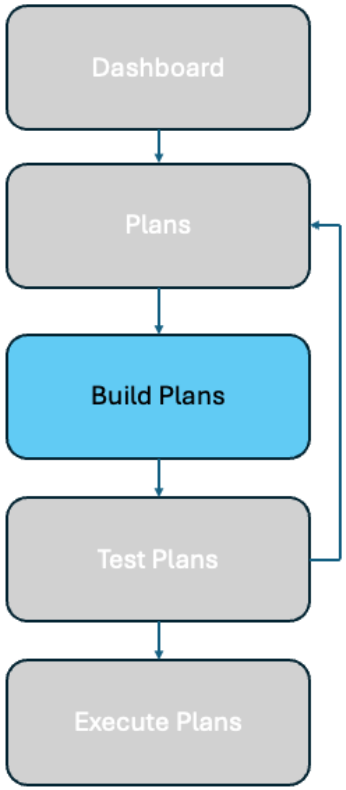
A new plan can be created using the “New Plan” button circled in red. Plans can be deleted via the trash-can button, highlighted in yellow. Additional task detail can be viewed by clicking the “Action” button on the main menu. And if modification are required click the “Re-Build” button highlighted in green. More on Build or Re-build in the next section.

Desktop View



Mobile View

Build a Plan



Building a plan

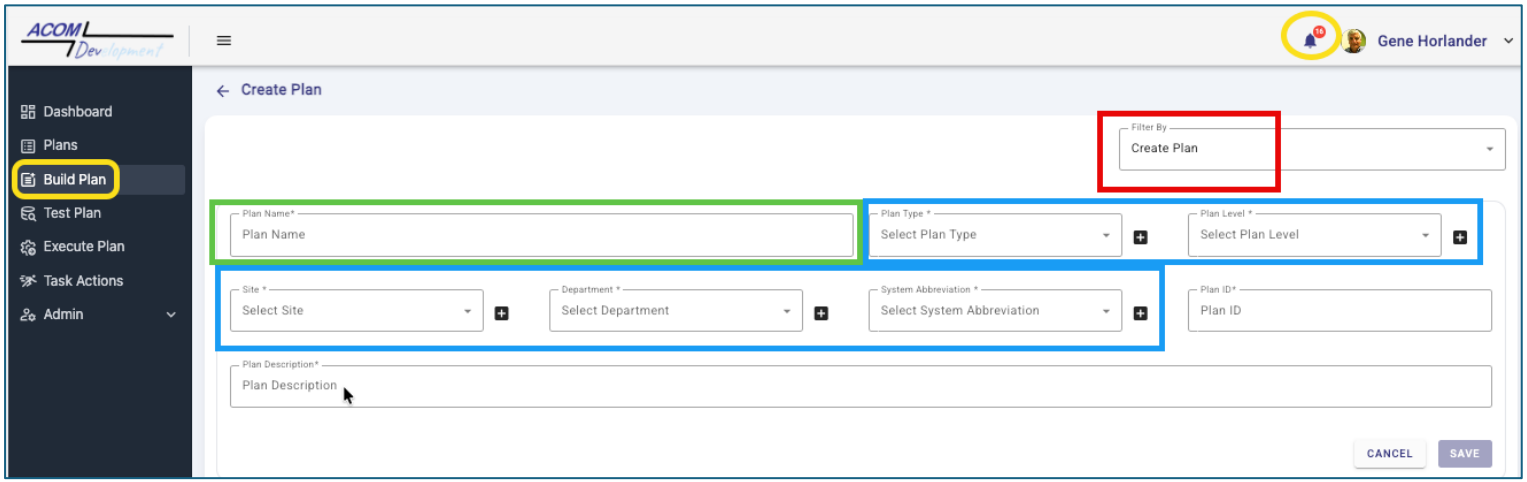
Building a plan in BPM whether it's for a disaster recovery, business continuity, cyber incident, emergency response by police and fire or military the overall concept and flow is similar. BPM houses a sequence of steps in a plan that will guide assigned users during a stressful emergency situations with clear instructions of each step sequentially dispatched in an orderly fashion.

The typical flow is **Build** a plan, **Test** a plan, then **Execute** a Plan. There is additional functionality for viewing plans in all stages, tracking activities using the dashboard, and administrative functions.

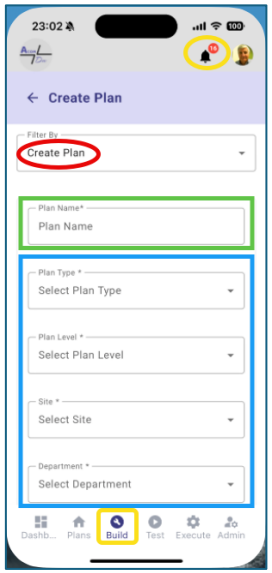
To create a new workflow/plan there are two options:

1) From the desktop version of BPM select the “New Plan” option in the “Plans” menu previous page, highlighted in red.
2) From both the mobile and desktop applications, select the “Build” menu, and choose “Create Plan” also circled in red.
3) Highlighted in yellow is a reminder icon, click this to see any outstanding messages from BPM.

Desktop View



Mobile View



Fields required to complete a workflow/plan are listed below:

- Plan Type, Plan Level, Site, Department, and System – *
- Description (500 characters)
- Creation Date (auto created)
- Last Modification Date. (auto updated)
- Plan ID (a computer-generated ID number)

* These fields can a be edited in the administrative section or during the creation of a plan by clicking the “+” shortcut button to the right of available fields allowing new values to be created on the fly.

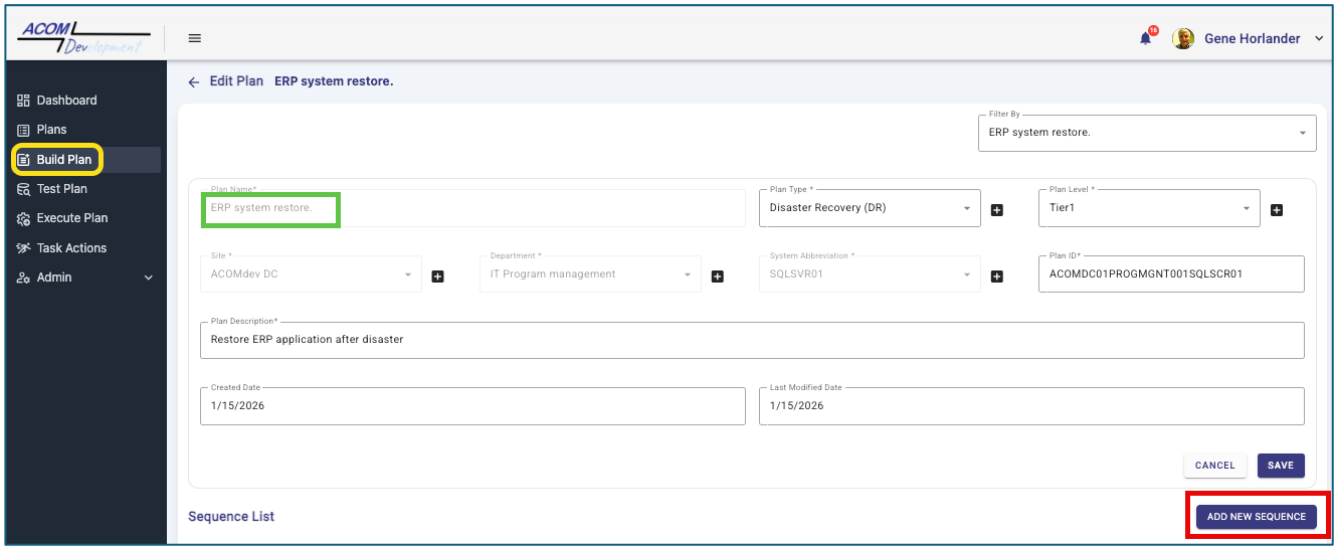
Adding a Sequence

BPM organizes plans made up of sequences and tasks. A sequence can be thought of as a group of tasks that must be executed in a sequential order. Each tasks dependent on the previous tasks.

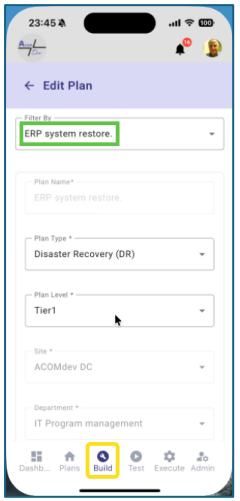
Groups of tasks that can be executed in parallel are managed by the creation of additional sequences (containers). A workflow/plan can have any number of sequences, and each sequence can have multiple tasks. When BPM executes a plan with multiple sequences it will dispatch tasks serially in each sequence, multiple sequences can be executing simultaneously.

Below is a newly created disaster recovery plan. Once the plan is created, various fields are used to document plan type, plan level, site (location), department, and system.

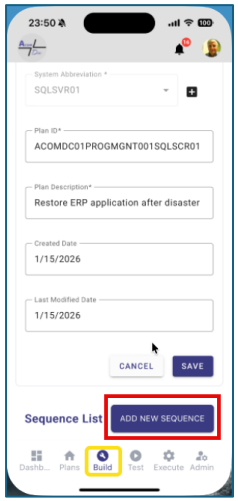
Desktop View



Mobile View #1



Mobile View #2



Adding Tasks

After a sequence is created tasks can be added.

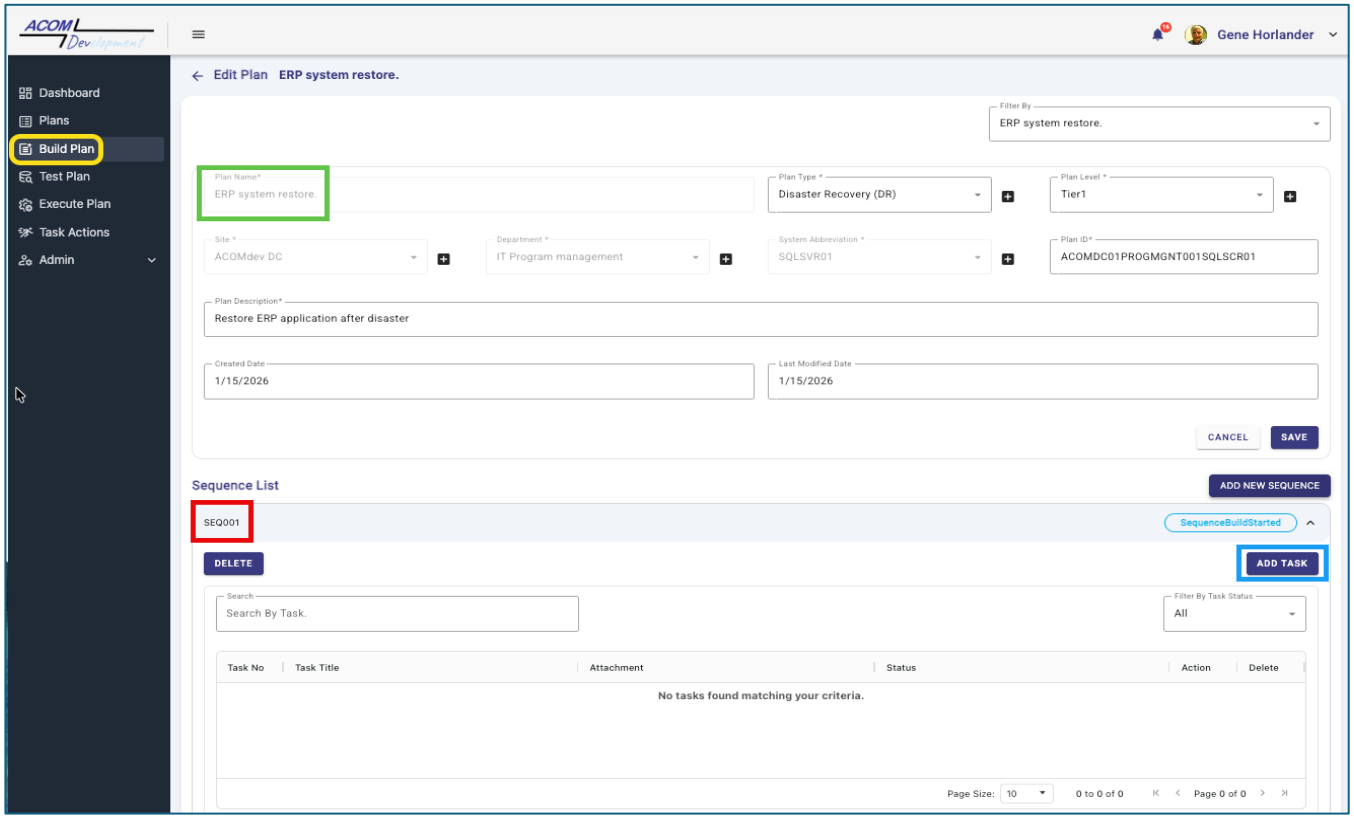
A task contains a description describing the work to be performed. A task identifies the primary team member assigned to the task; each primary team member will also have assigned a backup team member. Stored in the administrative section are all the details required to communicate instructions to both the primary and backup team members.

Task descriptions are included, in some cases the description is all that is needed, however, on more complex tasks BPM supports adding attachments. Most documents are supported: Word, Text, PDF, Excel, Power Point, Videos, and Photos.

The tasks are generally created by a subject matter expert with extensive understanding of the tasks to be executed during a disaster recover, as the task is created a time estimate is requested of how long these tasks should take. When a task is accepted by the team member the time estimate is used to track progress. Task execution time is tracked on the dashboard in real time allowing the team manger to monitor progress, if the actual time exceeds the estimate an alert is generated. The timing of task completion for a plan provides an indicator of overall plan completion. Typically, during a disaster recovery, timing of the recovery can mean the difference between thousands of dollars of penalties or lost sales.

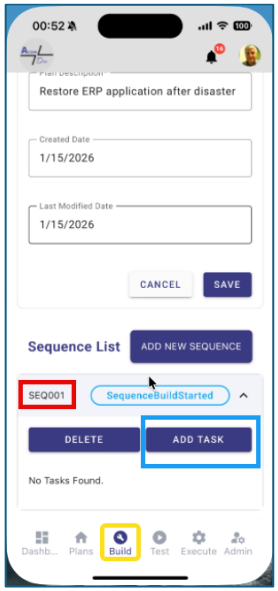
In the below screen, the plan has been completed, with sequences, and now tasks creation is next. In this plan we created one sequence, SEQ001 (highlighted with red), now to add tasks click the “Add Task” button, highlighted with blue.

Desktop View



Mobile View #1

Mobile View #2



The Plan name is outlined in green, sequence name with red, and the button to add a task is blue.

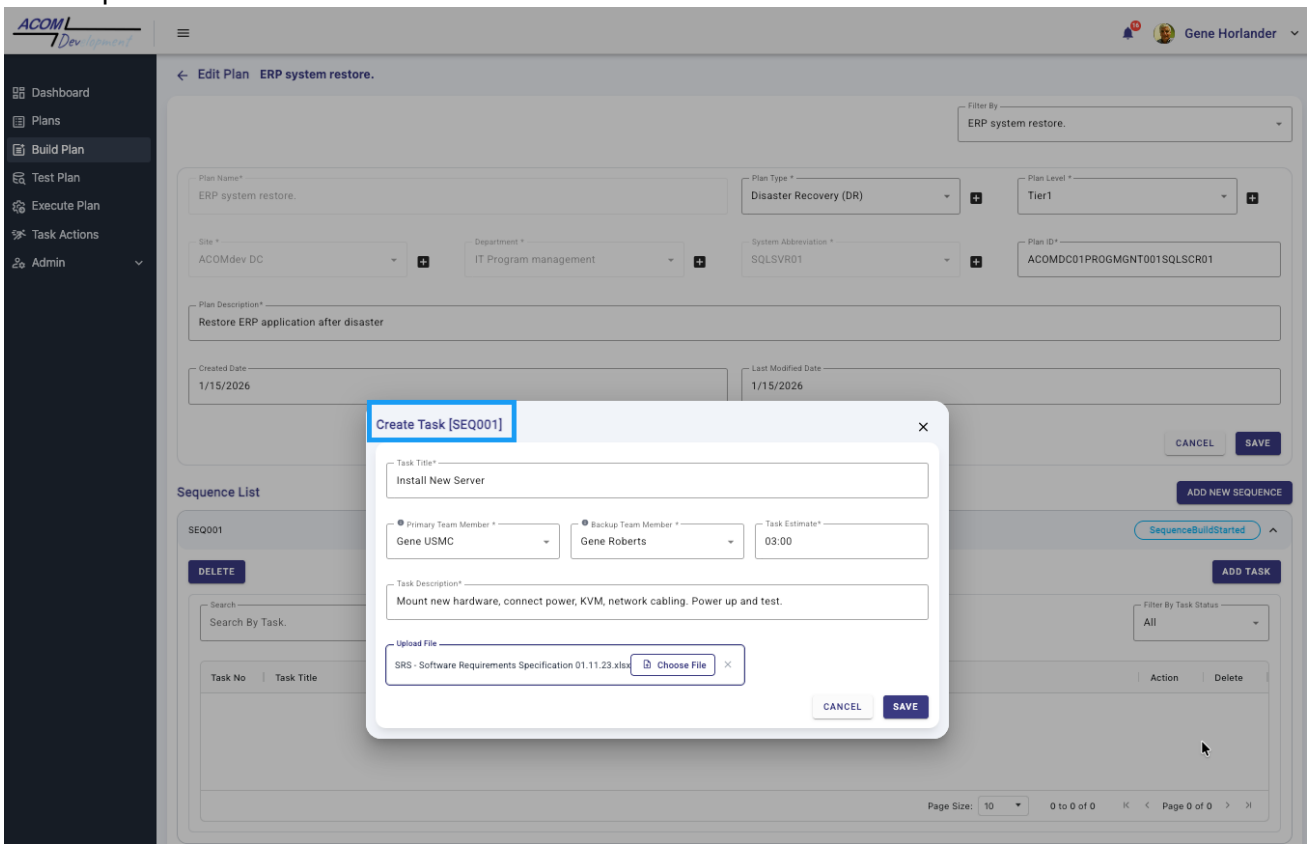
A best practice: While building plans, click “Save” often.

Adding Tasks Details

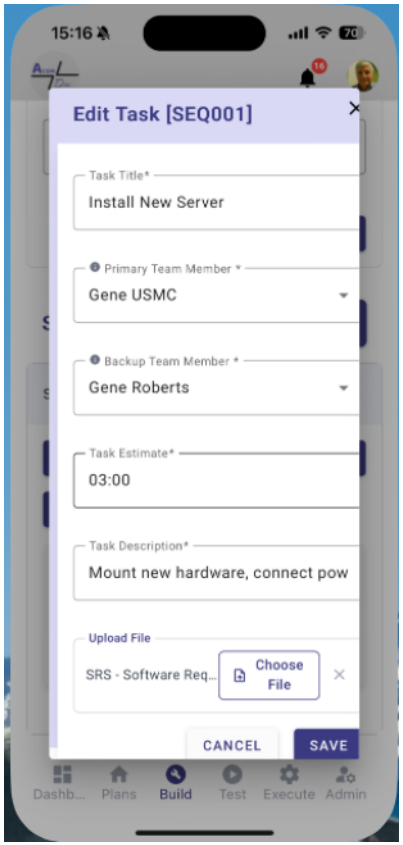
Click on the “Add Task” button, highlighted in blue. The below window opens ready to accept tasks details.

Task T1 – Install New Server

Desktop View

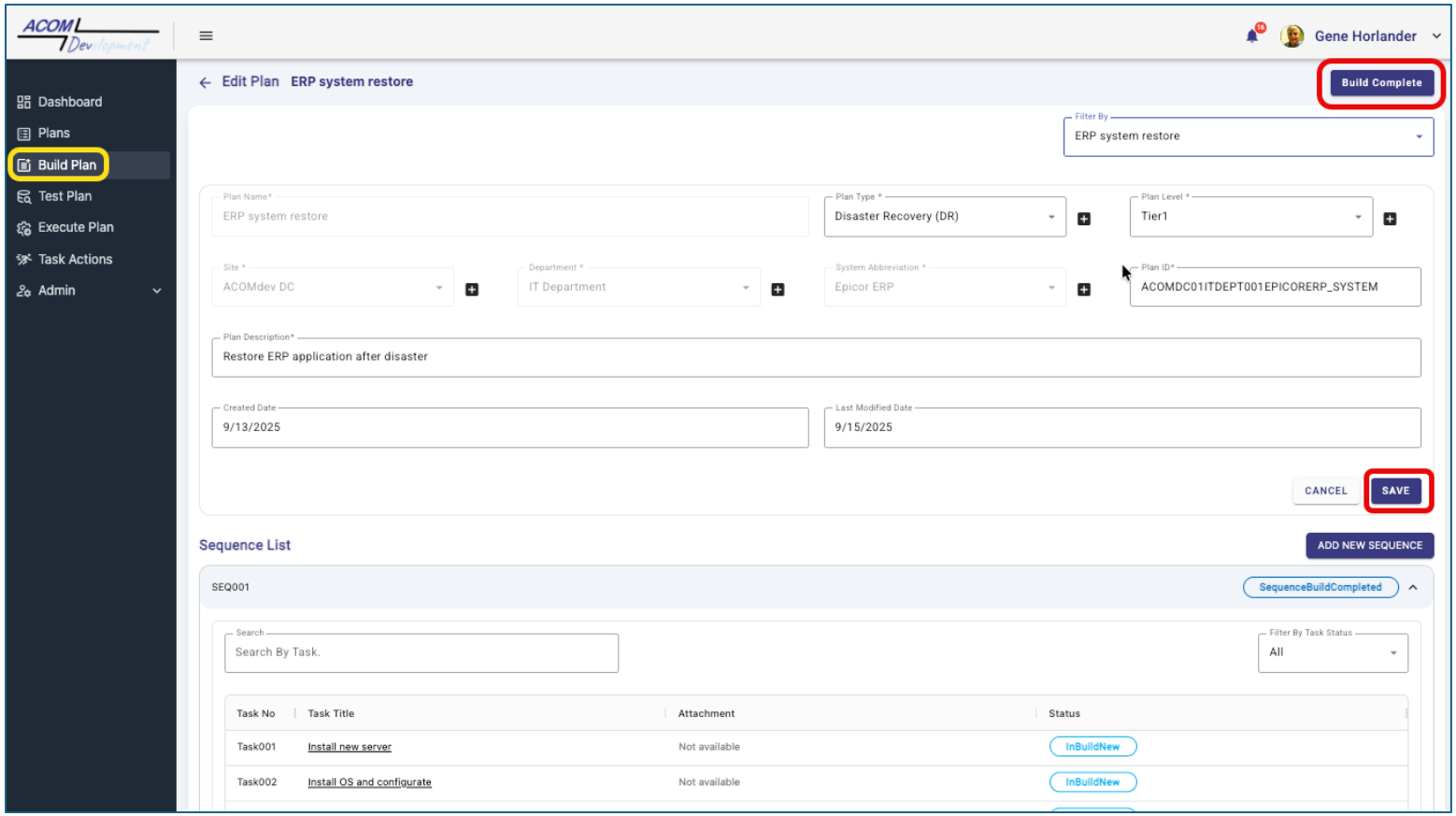


Mobile View

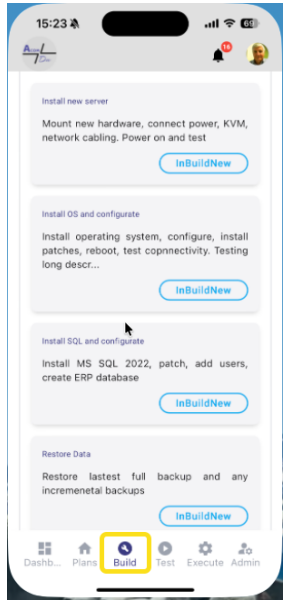


Completed Plan - Build Complete

Desktop View



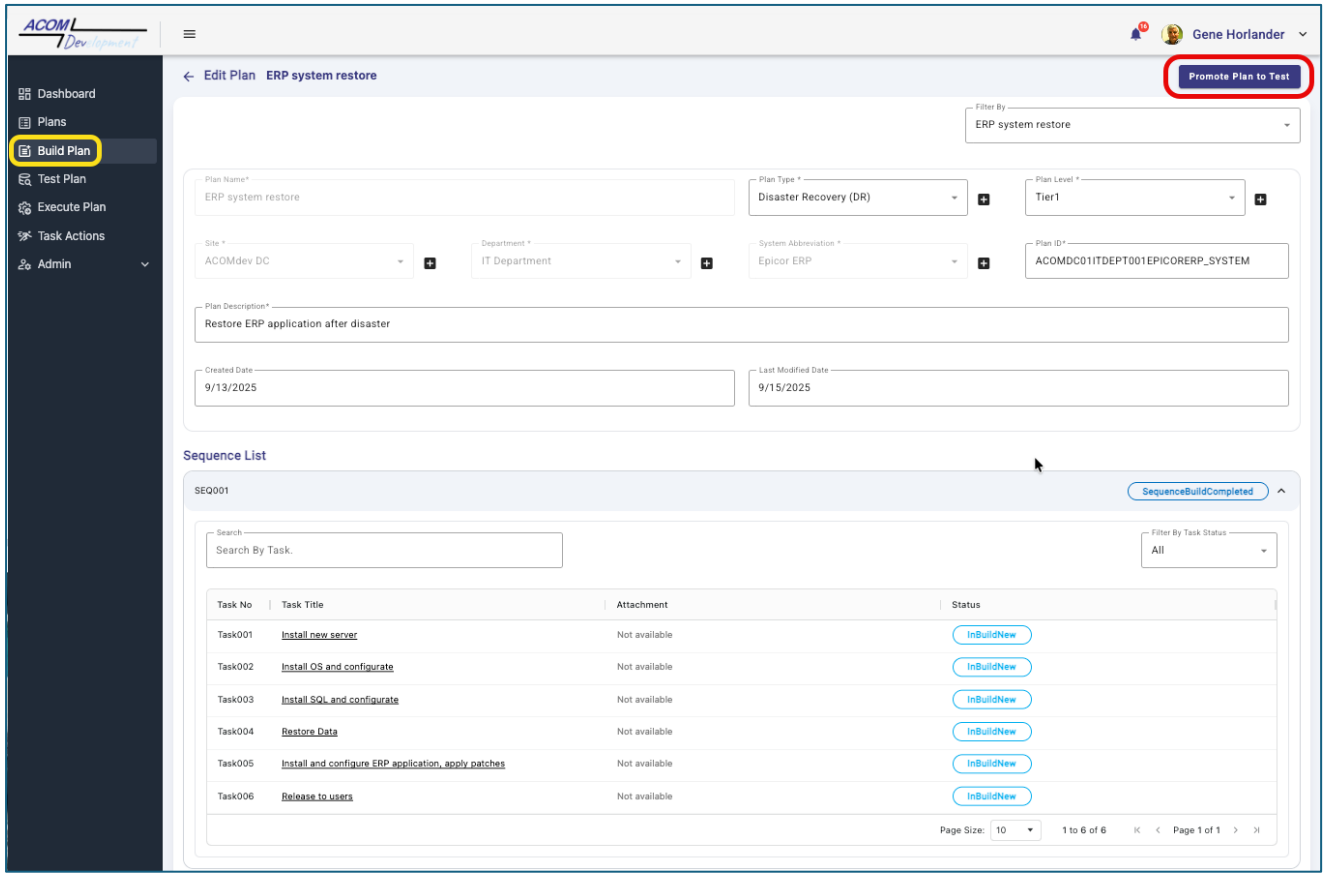
Mobile View



Assuming no other sequences are desired, or tasks, at this point to complete the build process click “Save” then “Build Complete,” circled in red. If more sequences are desired after testing, the plan can be edited. After saving you are presented with an updated screen that includes a button at the top of the screen called “Promote to Test”.

Completed Plan - Promote to Test

Desktop View



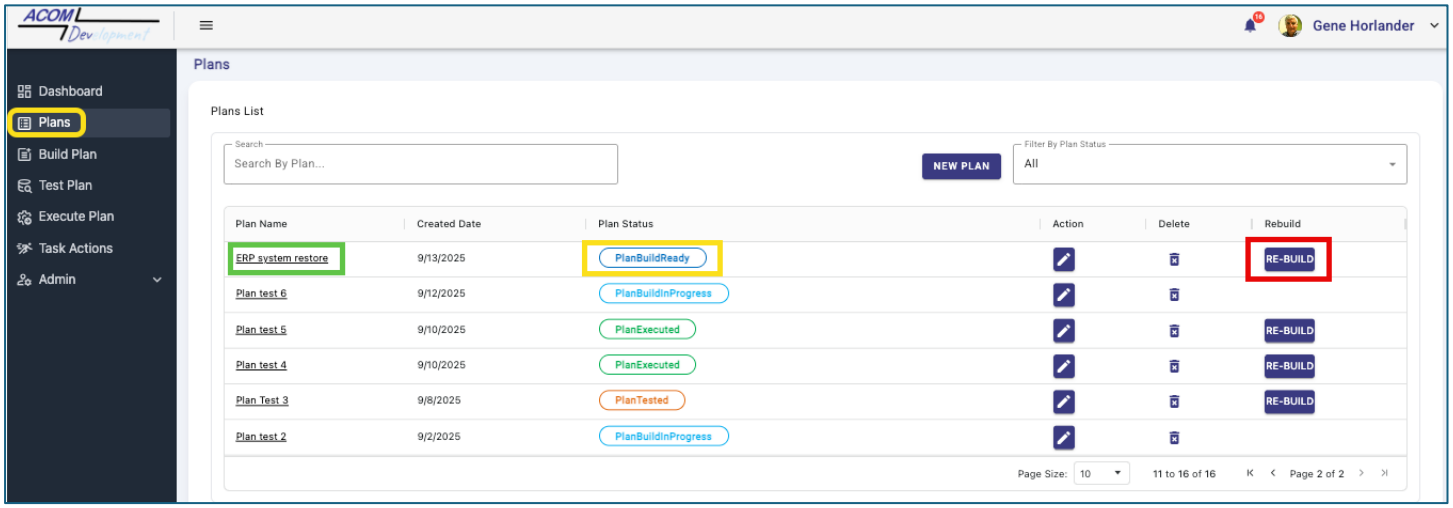
Mobile View

Last step is to click on “Promote Plan to Test.”

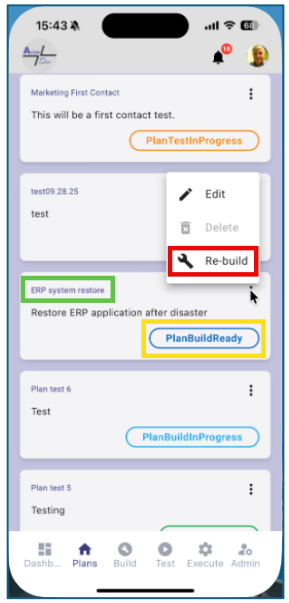
At this point the plan status has been updated to "**PlanBuildReady,**" and the plan can be scheduled for testing.

Note: the "Re-build" option allows making changes if required after testing. Sometime testing revels changes or modifications that are needed. This option allows modifications to an existing plan.

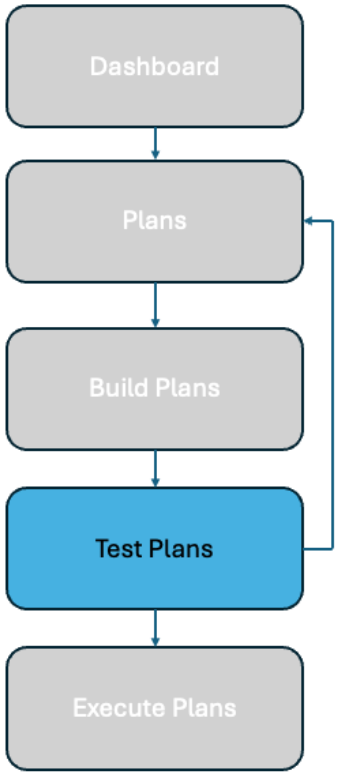
Desktop View



Mobile View



Test a Plan

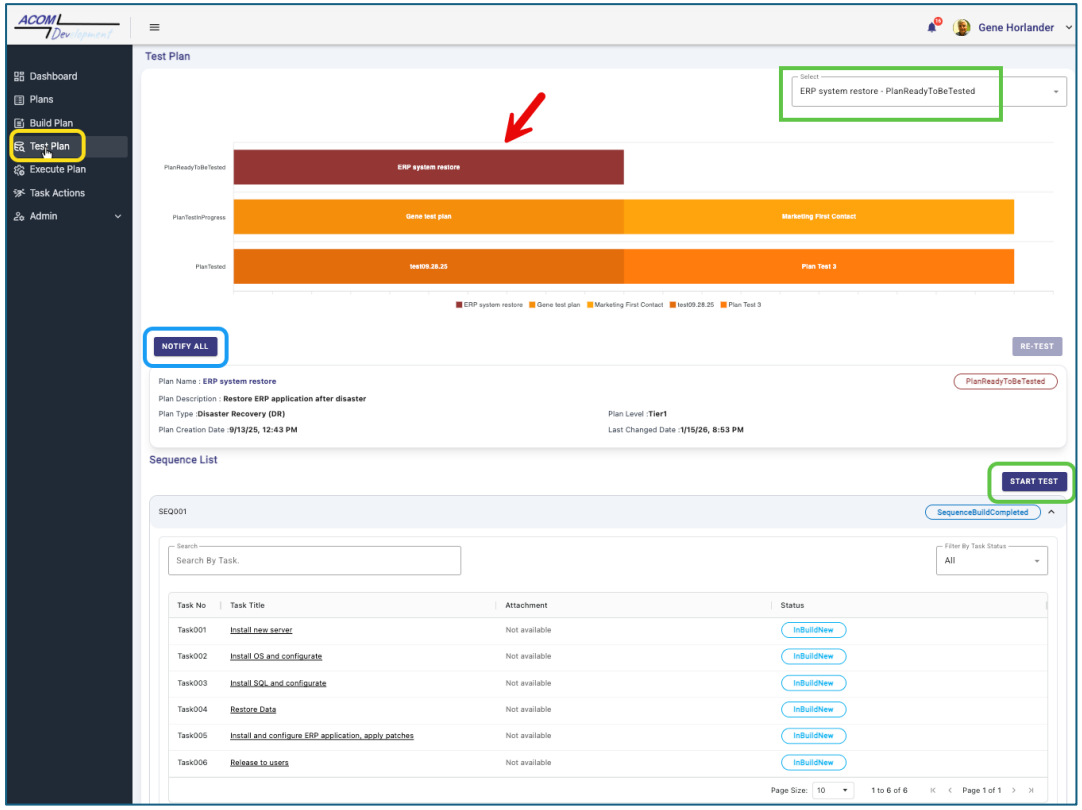


After a plan is built. Any plans that are ready for testing will appear on the “Test Plan” menu screen.

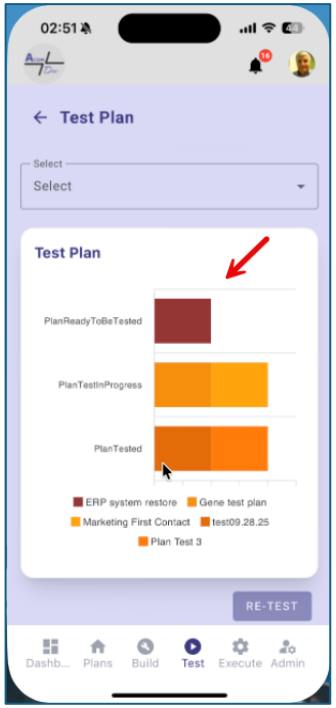
- Plans Ready to be Tested
- Plan Test in Progress
- Plans Tested

Test Plans Menu

Desktop View



Mobile View



Select Plan to be Tested

Click on the workflow/plan “ERP system restore” from the “Plans Ready to be Tested” category, on the **Test Plan** screen. Selecting the plan loads the sequence(s) and tasks.

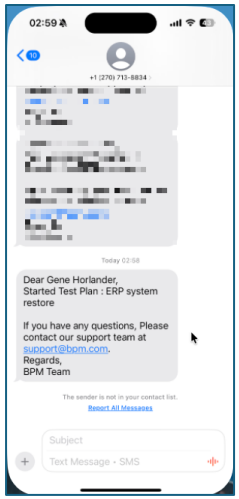
A **good practice** before starting a test is to notify all users that a test will be starting with the “**Notify All**” button, blue circle on the “Test Plan” menu on previous page - click “Notify.”

When ready click the “Start Test” button, on the **Test Plans** menu (previous page), circled in green.

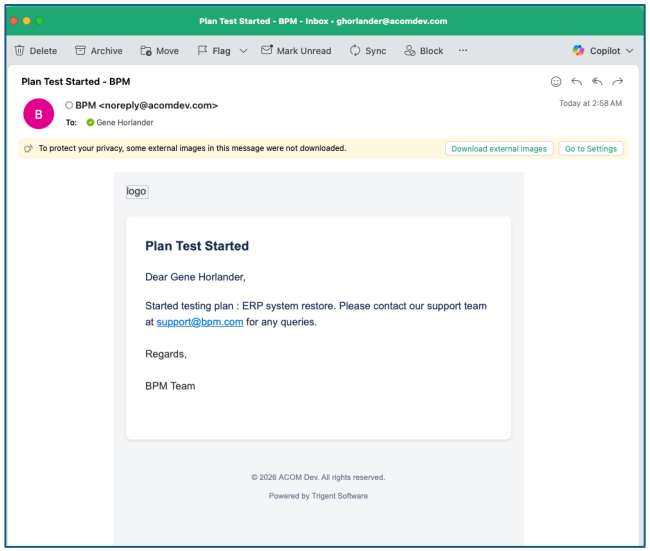
Notify Team Members

All team members, including managers and directors that have been assigned as participants in the plan will receive the same notification via email and text. Note: in this example, the Team Manager - Gene Horlander received a text via an Apple iPhone and Outlook email notification.

Mobile Text Notification



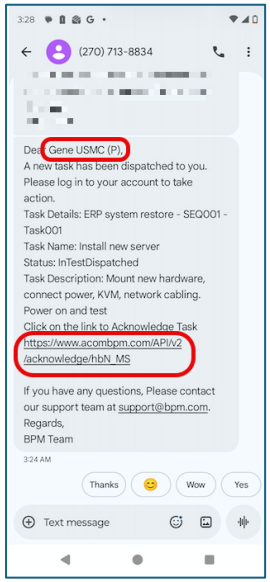
Desktop Email Notification



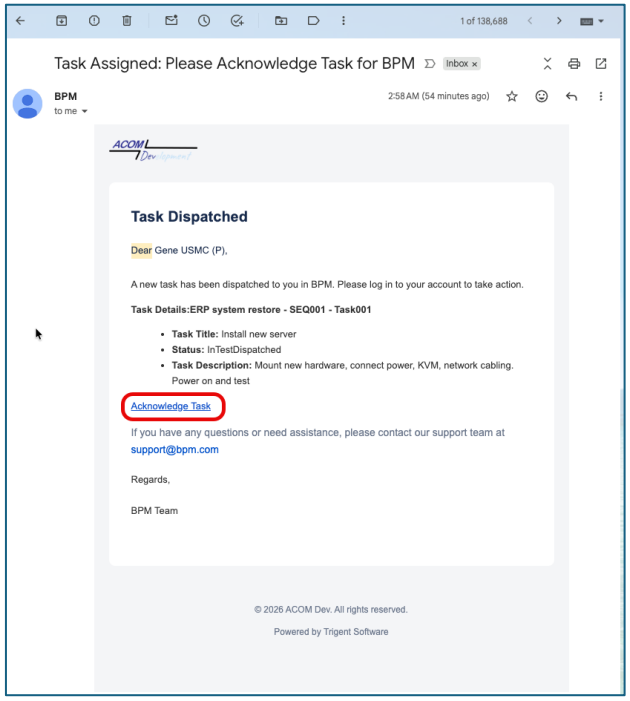
Team Member receives task update

The Team Member - GeneUSMC received a Task #1 text notification (left image) and via email. Note, his mobile device is an Android phone and email is Gmail. Gene's email address also contains an identifier (P), meaning GeneUSMC is the primary assignee of this task. The Backup Team Member will also receive a copy of all text sent. The text on the right to the backup team member Gene Roberts, note next tohis name is the designation (S), for secondary or backup.

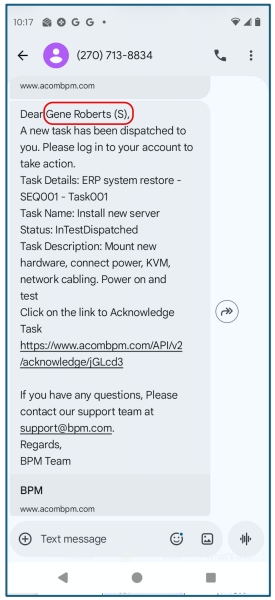
Mobile Text Primary



Desktop Email Notification



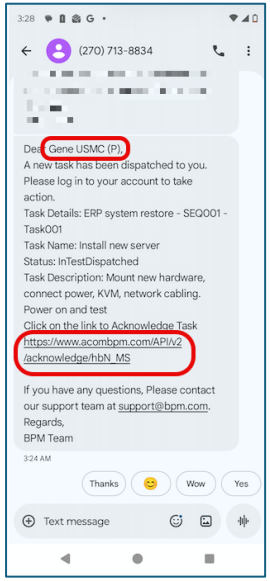
Mobile Text to Backup



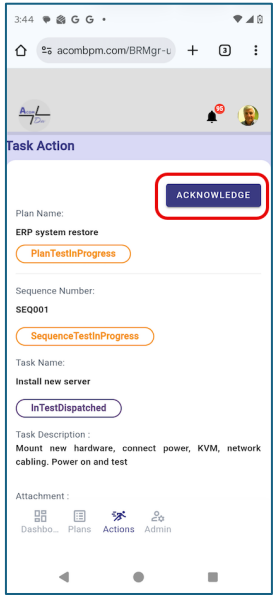
Task Accepted

GeneUSMC clicks the link in the text to accept the task on his Android phone and is then routed automatically to the task in the BPM application to complete the acknowledgement (right image).

Mobile Text Notification



After clicking link, user is routed to BPM to confirm task acceptance.

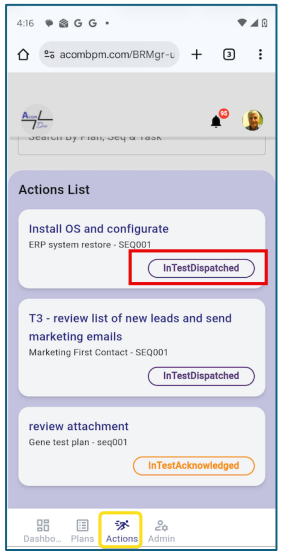


Task Completion

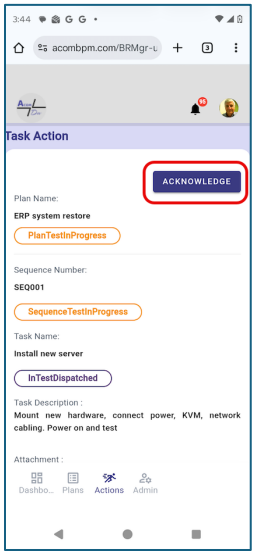
During the activities associated with a disaster recovery or any plan execution, as technicians are working to complete a task mobile device(s) may time out, thus getting back to the right sequence in BPM can be confusing.

BPM allows for these situations, during the execution of a plan sequence an additional menu item will appear titled "Actions." Click on "Actions" anytime to return to the last open task activity. On the left image below notice multiple open tasks items, this exercise is testing the plan "ERP system restore," and still preforming task within the sequence SEQ001, and currently on Task 1 "Install new server." The function "Actions" will show the most recent open task at the top of the list, "ERP system restore." Click on the status highlighted in red – InTestDispatched, and BPM resumes. Now, GeneUSMC can click "Complete."

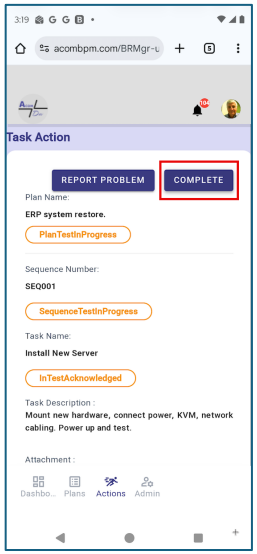
Mobile Action to resume



BPM resumes task

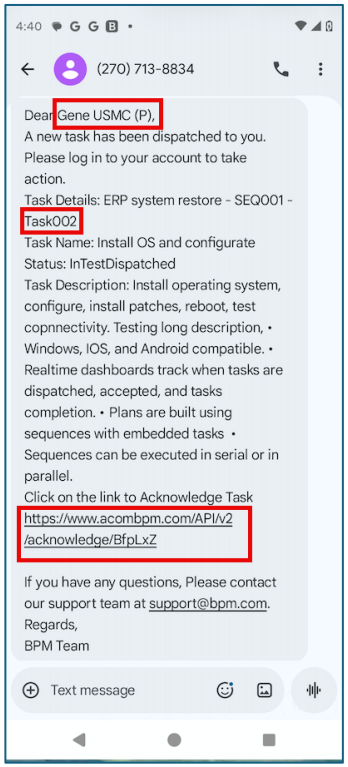


Click Complete when finished

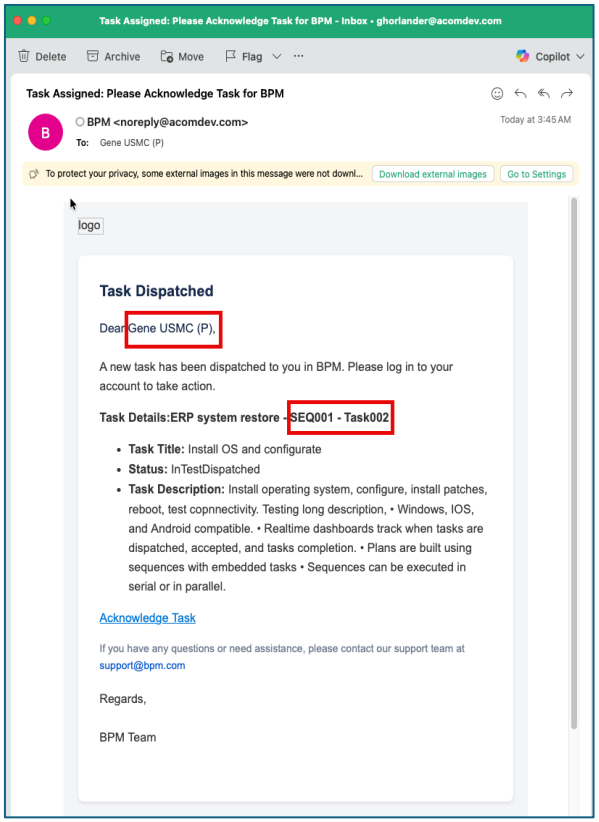


When a task is completed, BPM dispatches the next tasks.

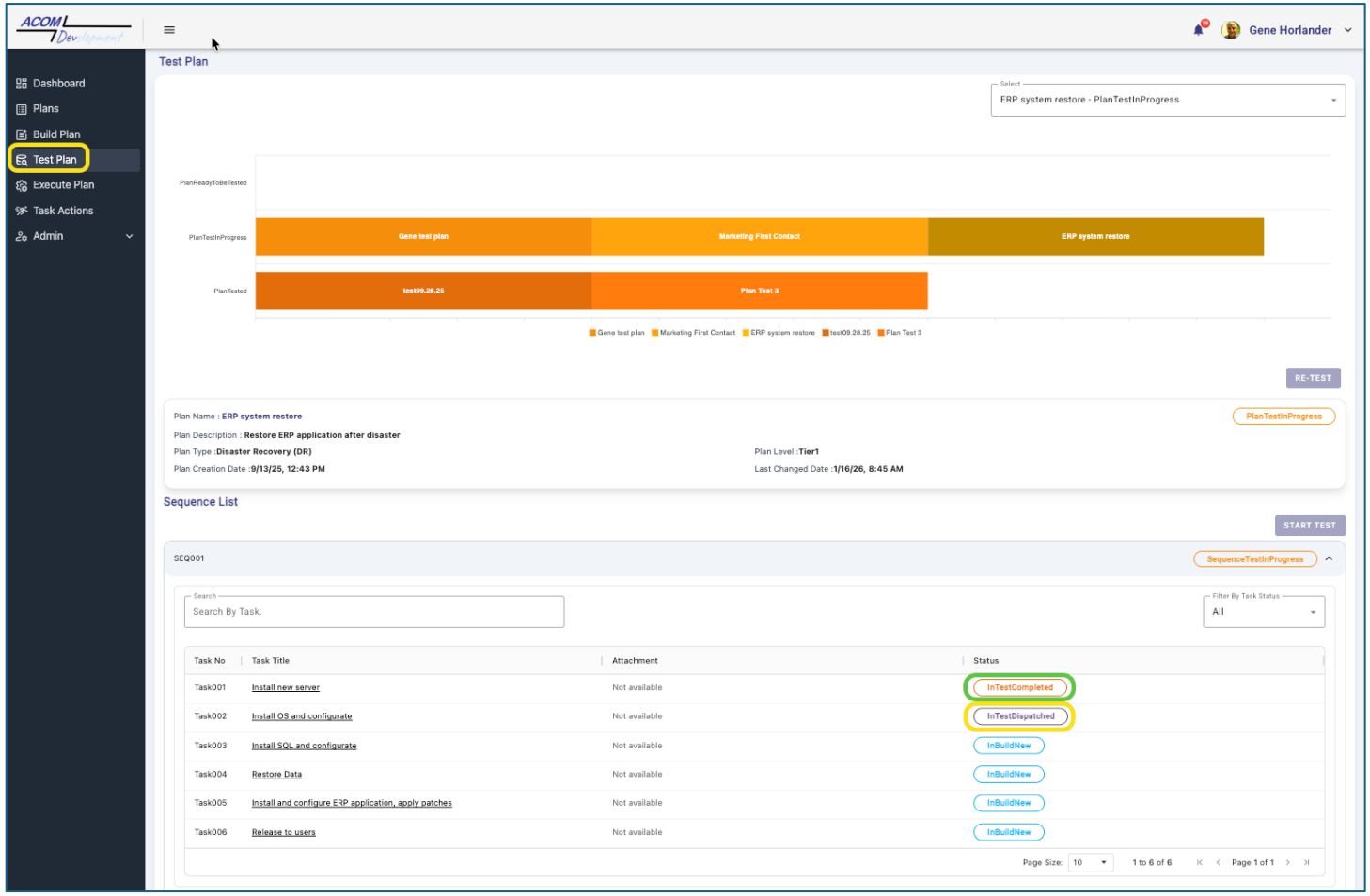
Mobile Dispatch Task #2



Email notification for Task #2

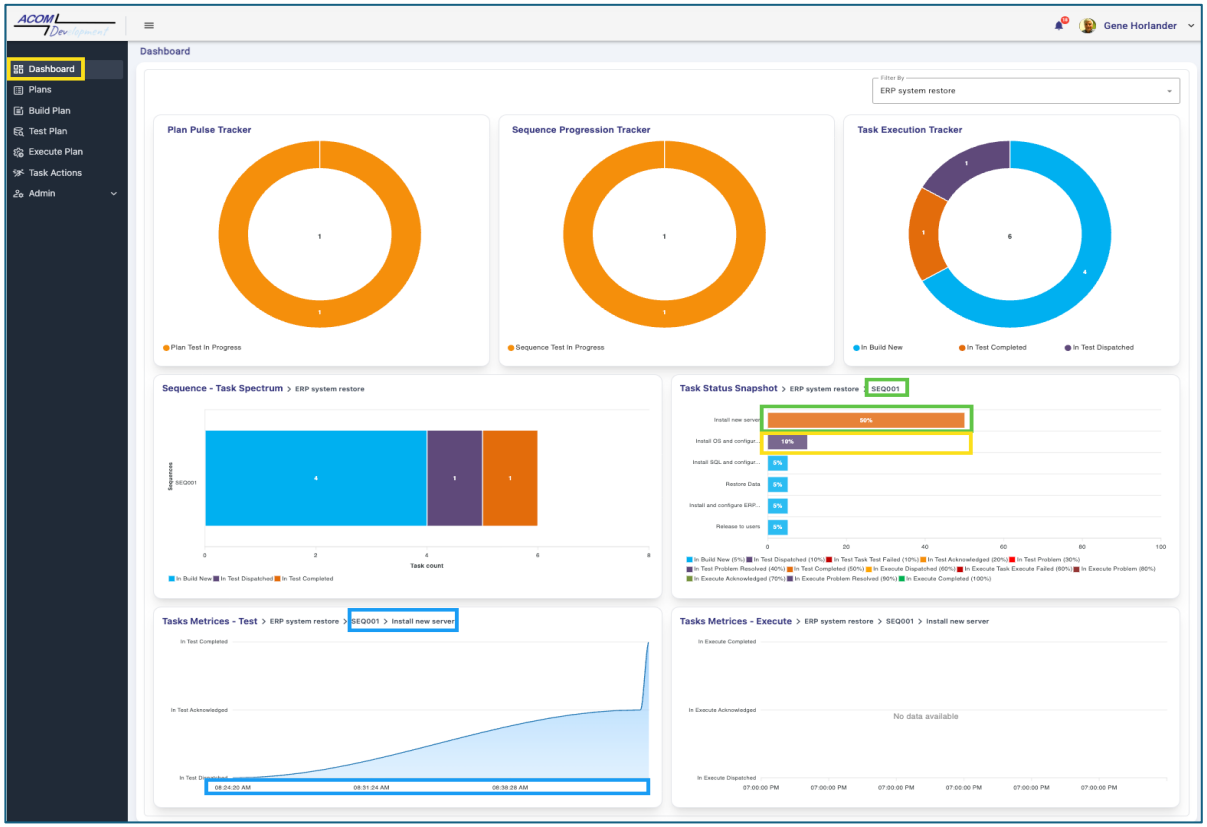


Go to “Test Plan” menu for status of tasks, note as task are being executed status is updated and displayed. Task #1 is marked “InTestCompleted,” and Task #2 “InTestDispatched.”



Dashboard - Task Status (real-time)

Dashboard – Plan “ERP system restore”



Notes

Task #1 in SEQ001 marked complete – green box.

Task #2 in SEQ001 is dispatched – yellow box.

Task Metrics for Task #1 show the following time increments – blue box:

Dispatched
08:24:20

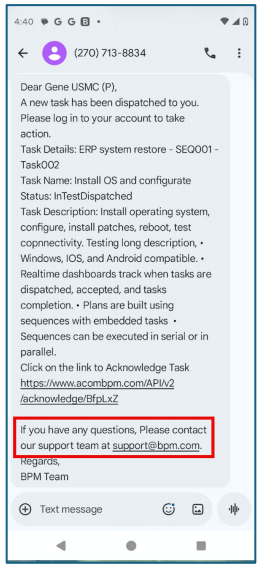
Acknowledged 08:45:06

Completed
08:45:32

BPM dashboard tracks every plan, sequence, and tasks activities and time stamps. This information is logged to the audit file and used for Power BI reporting. The time logging is real-time, allowing teams to compare and verify time executions. Since the dashboard is available to all users, it can also be used to monitor a disaster recovery plan in progress.

Problem Alerting

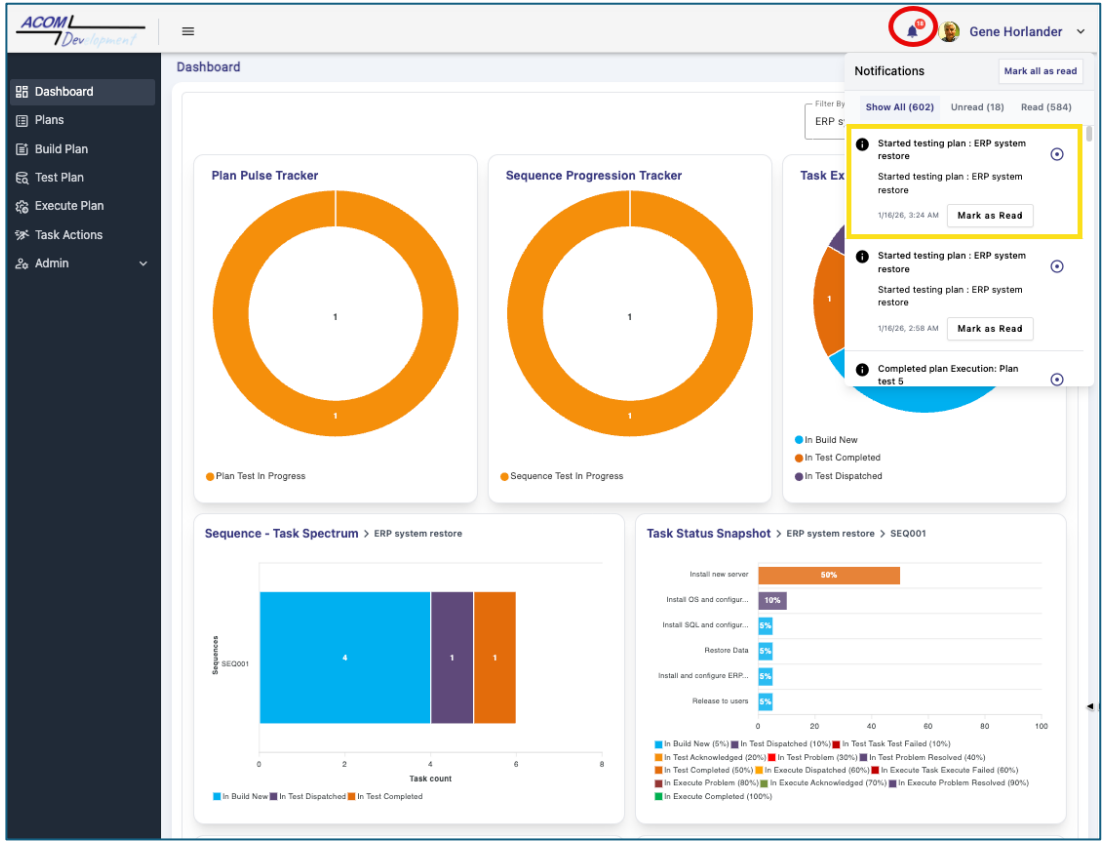
During the execution of tasks should a problem develop preventing a team member from completing the task, the user can click on the support@bpm.com link to alert management of issues. Each task dispatched contains a support/help alert link.



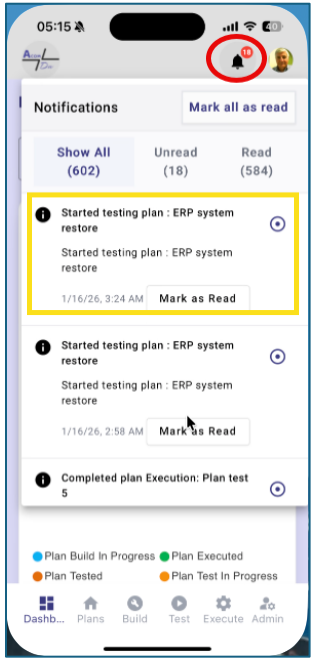
Reminders / Notifications

Please note, task reminders are also dispatched periodically via text and email. To view alerts or reminders click on the “Bell” icon see the upper right-hand corner highlighted in red.

Alerts / Notifications
Desktop View



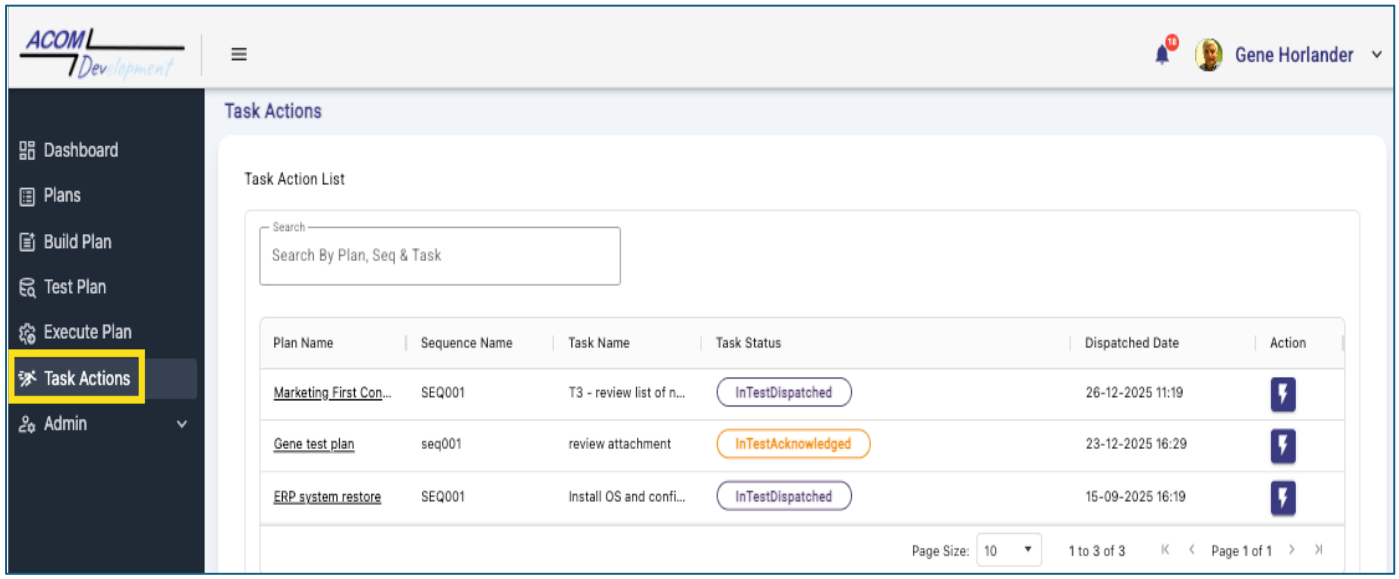
Mobile View



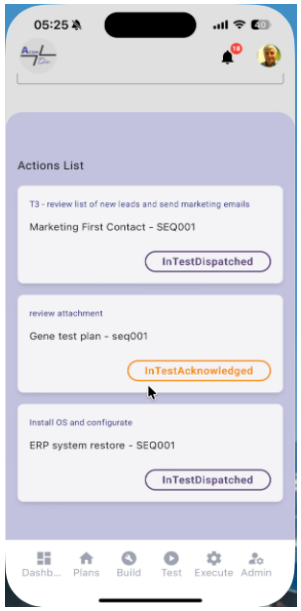
Task Actions

The “Task Actions “options are available anytime from the admin menu or during plan execution. During plan execution BPM enables the menu item on the left menu.

Desktop View – Task Actions

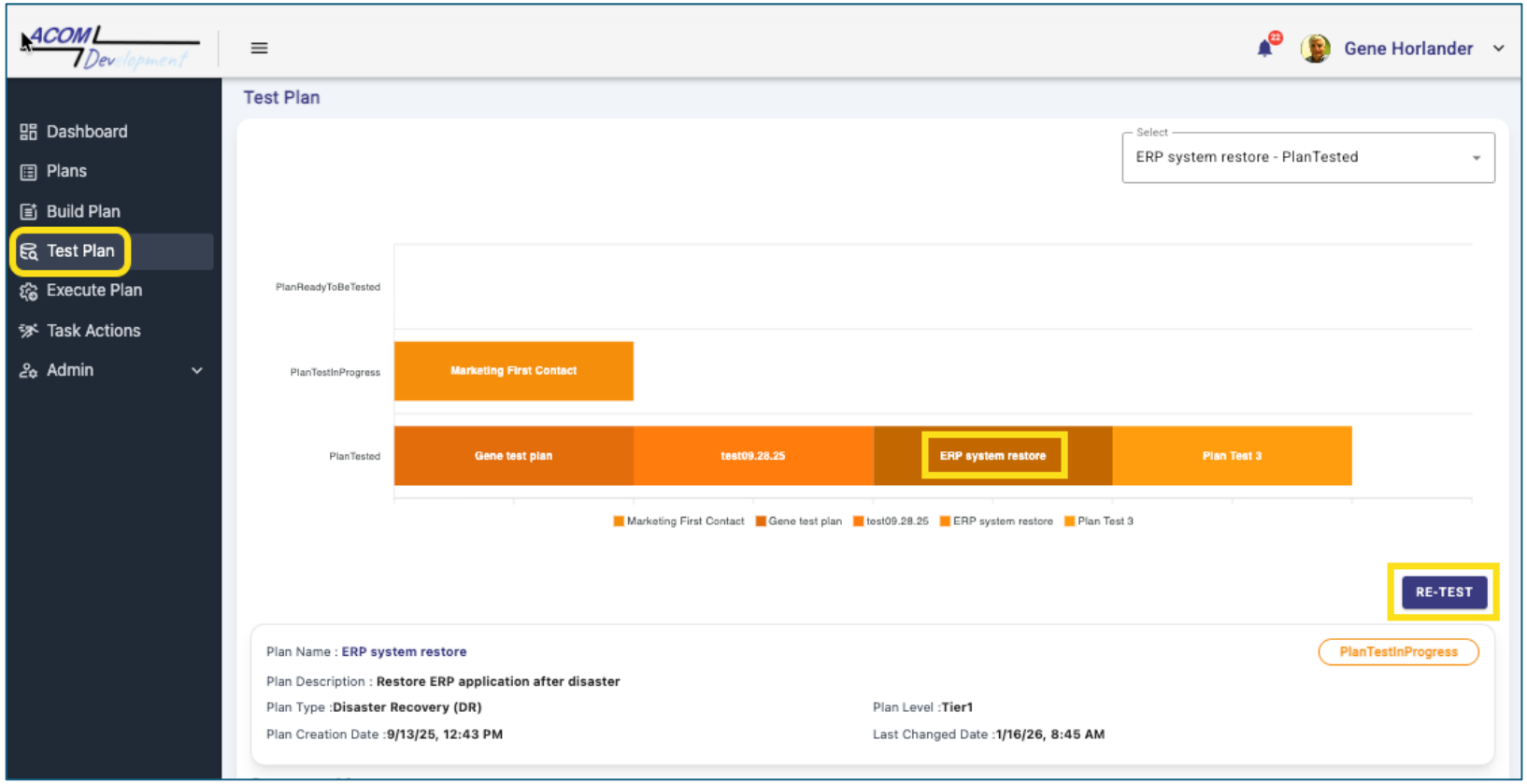


Mobile View



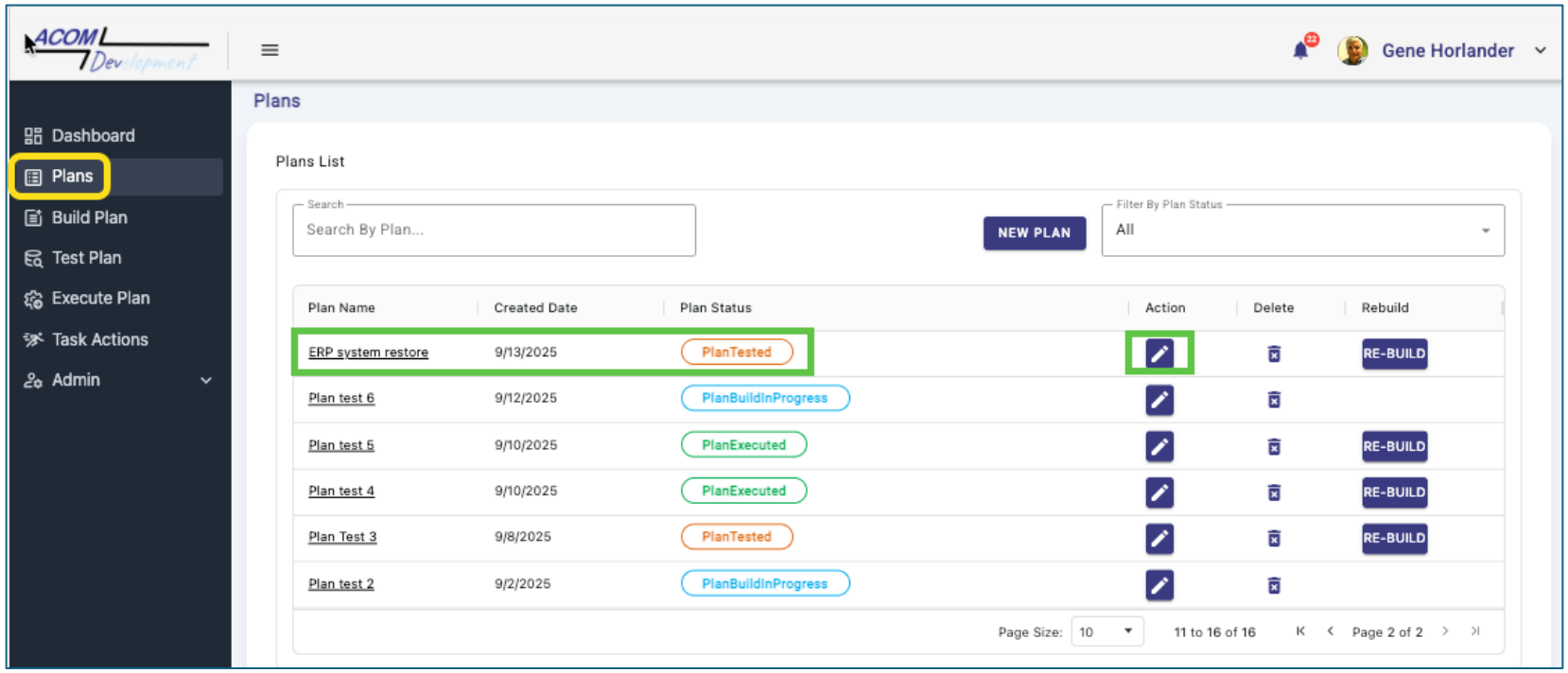
Retesting

The Plan can be tested again by clicking on the “Re-Test” button, highlighted in yellow.



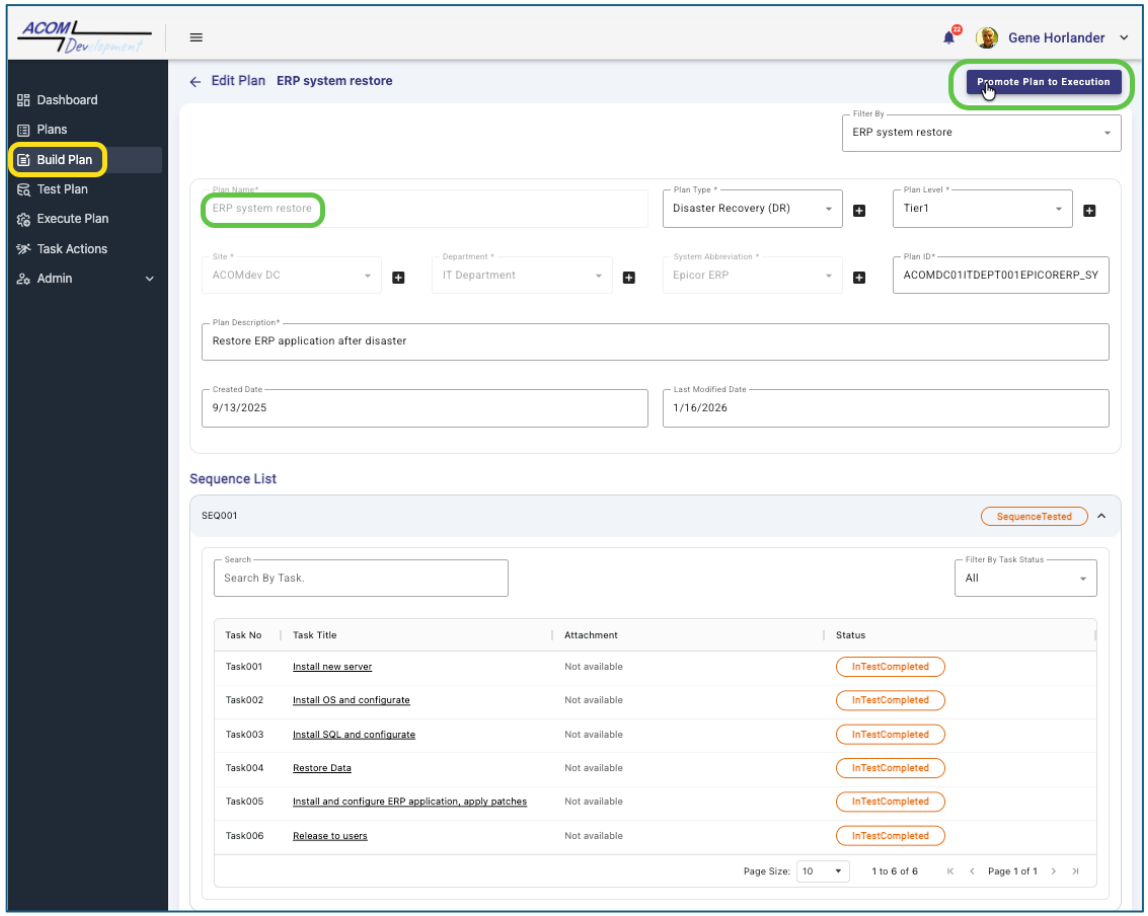
Workflow Promoted to Execution Status

Viewing the “Plans” menu, the “ERP system restore” plan is Complete with status of “PlanTested.” Plan can now be promoted to “Execute Status” by clicking the “Action” button.

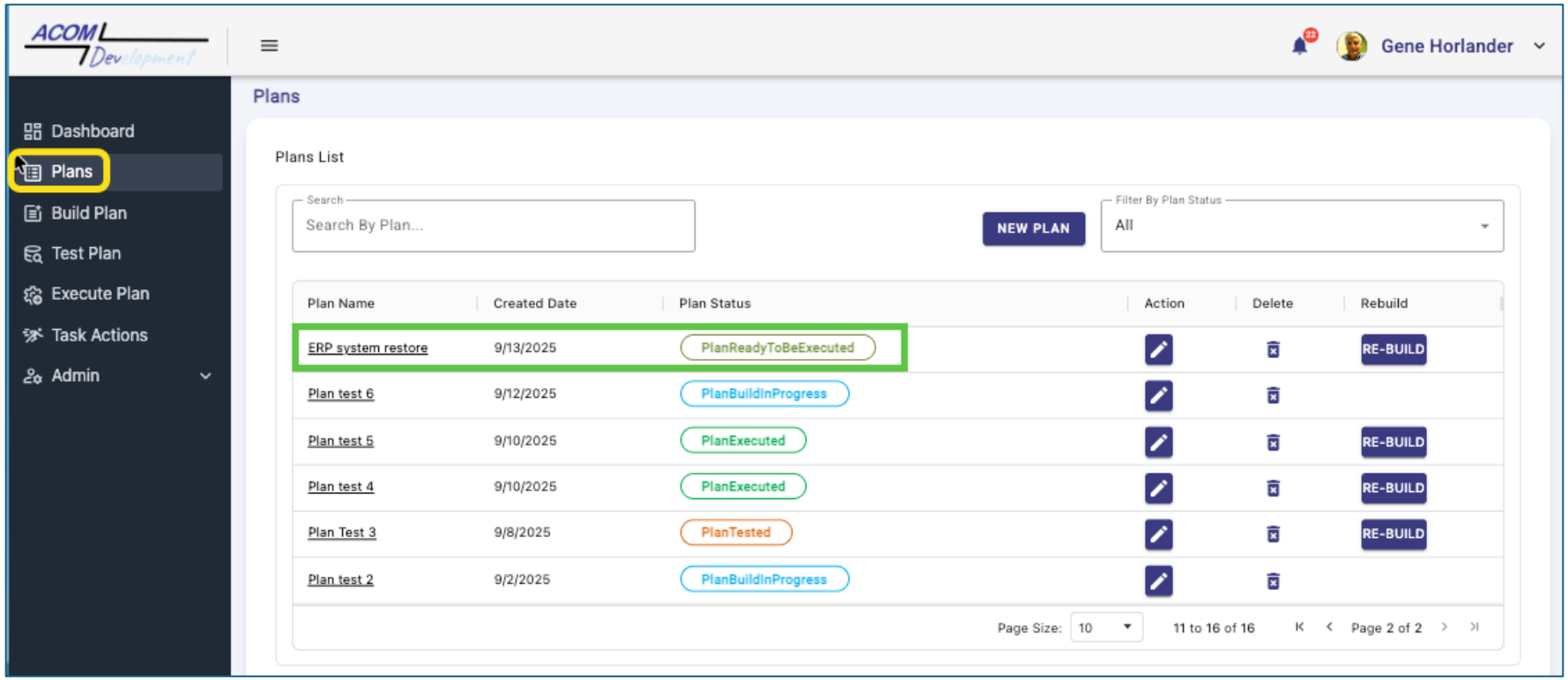


Approve and Promote Plan

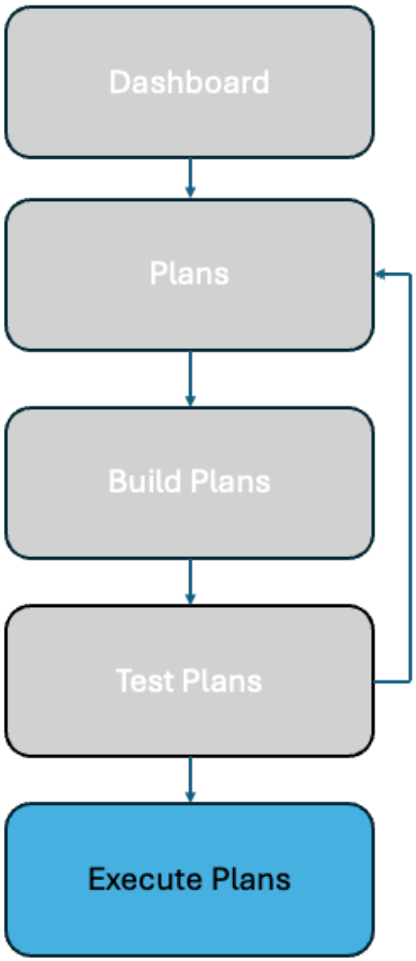
Clicking the Action button brings up the “Build Plan” menu, and the disaster recovery plan can be promoted to execution status by clicking “Approve Plan” highlight by green box next slide.



View “Plans” menu, plan is ready to be executed.



Execute a Plan

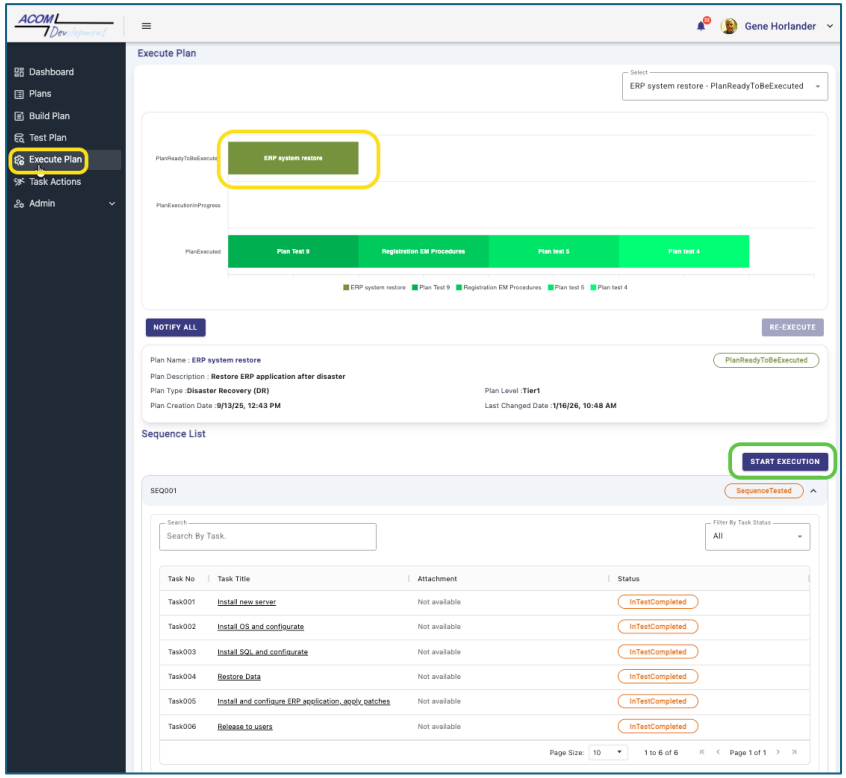


Execute a Workflow/Plan

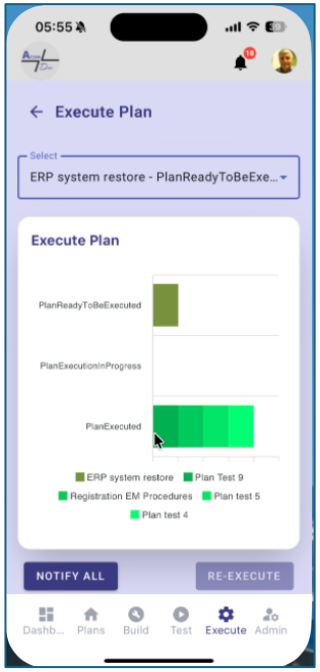
The execution process for a workflow/plan in BPM is almost identical to the test execution, so no need to go through this again in detail. BPM allows all plans to be re-executed with no limit; there is also no limitation on the number of plans.

Shown below is the “Execution Plan” menu. The recently tested plan “ERP system restore” has completed testing, is approved, and has been promoted to Execution. To start an execution, click on “Start Execution” button. Team members can be alerted in advance using the “Notify All” button, as before when testing.

Desktop View



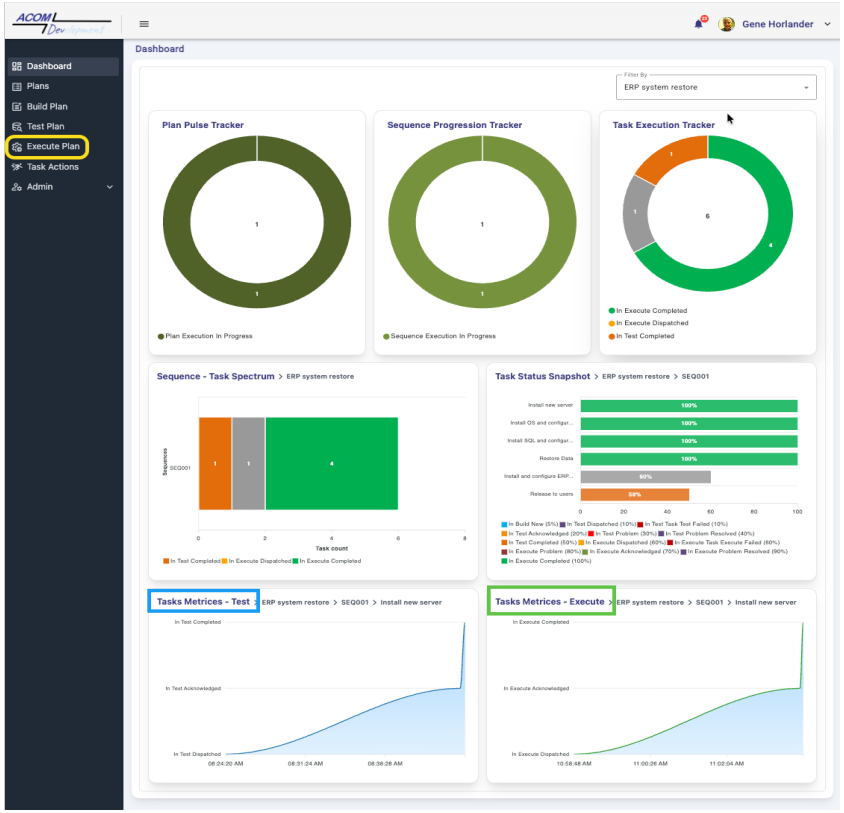
Mobile View



Workflow Execution Dashboard Metrices

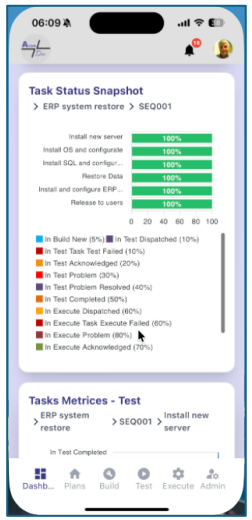
Dashboard view of Disaster Recovery plan “ERP system restore” showing overall task snapshot data, “testing” metrices bottom left (blue), and “execution” metrices bottom right (green).

Dashboard View



Mobile View

Task status snapshot



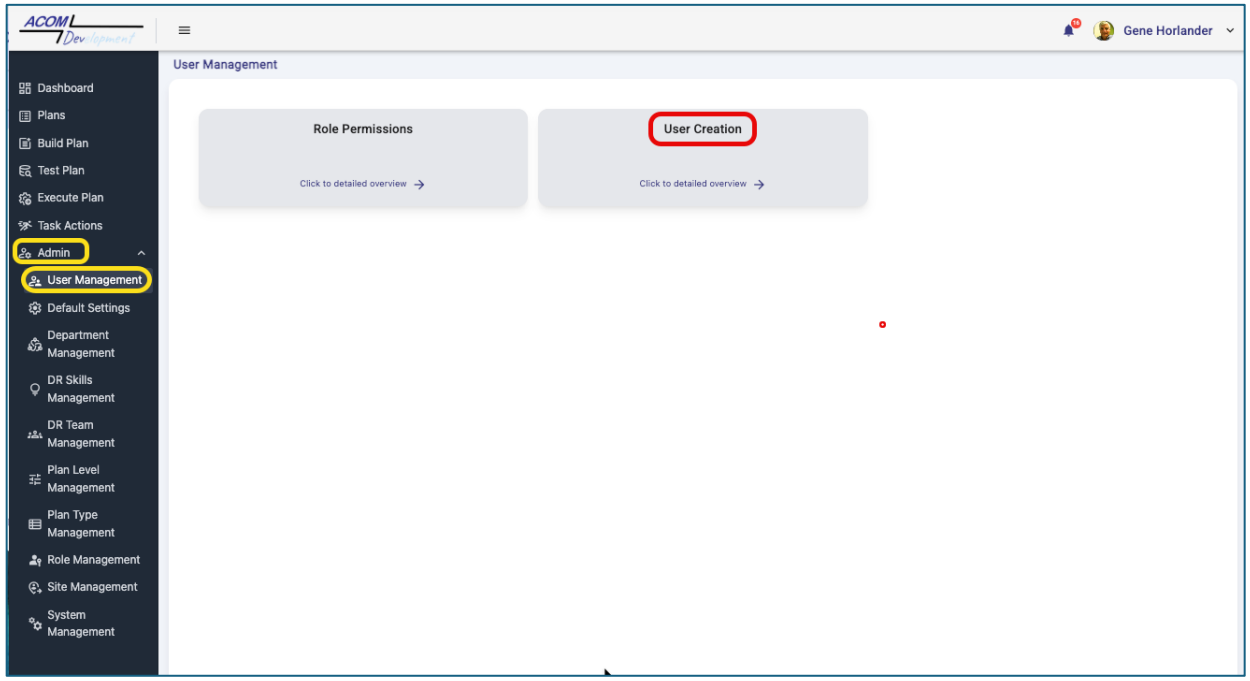
Test Metrices

Execution Metrices

Administrative Section

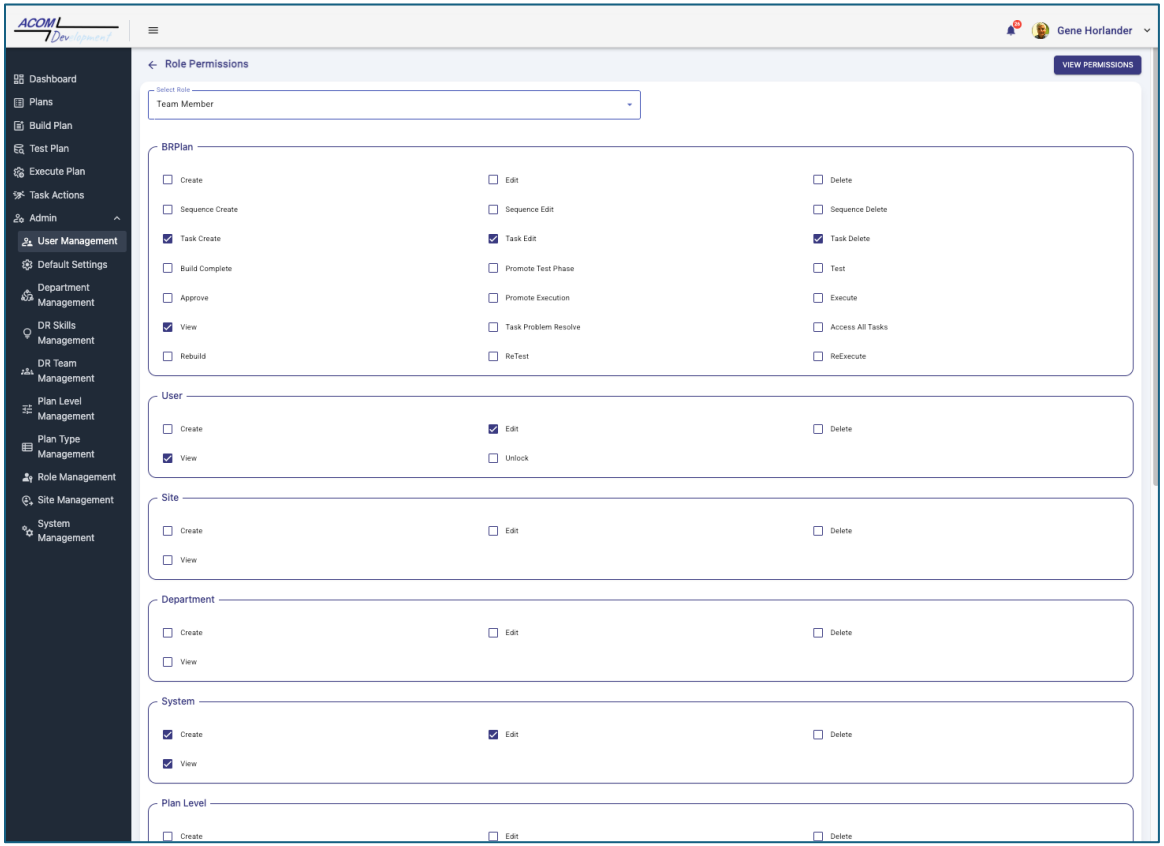
User Setup

Add users … BPM is free for the first 5 users. To add a user, select Admin from the main menu, then User Management, and then User Creation.



When creating a user account, there is also a menu option for Role Permissions,

For now, you can bypass Permissions and use the default settings. Going forward as your requirements become more complex permissions is an extensive area of policy management with an array of rules that allow extensive control and fine tuning of user's access and capabilities in BPM.



Role Permissions: (view only)

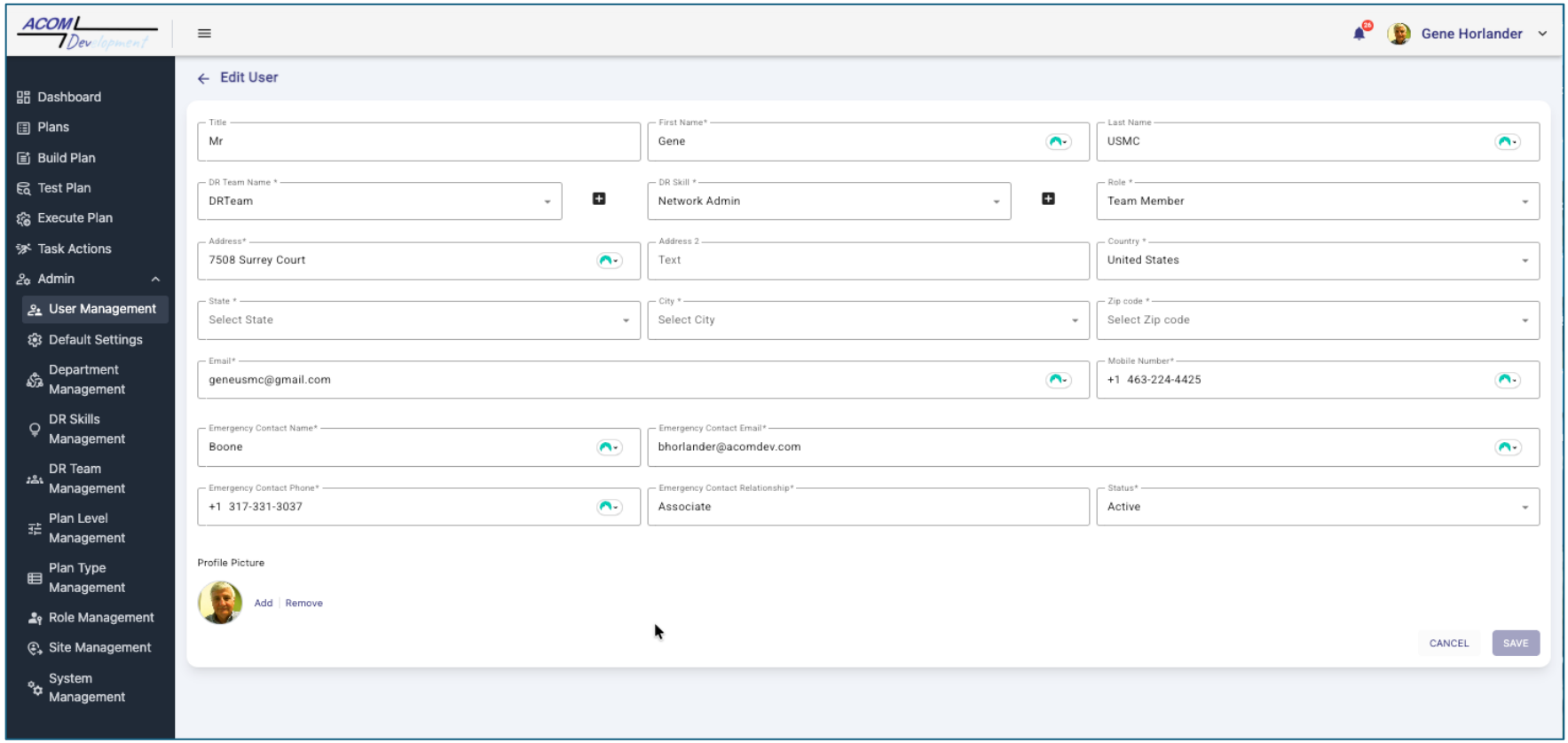
Select Role: dropdown.

Displays:

- BRPlan
- Site
- Department
- System
- Plan Level
- Plan Type
- Other
- Default Configuration
- DR Skill
- DR Team
- System Type
- History/Log (system only)

Adding Users:

Adding a user is a straightforward process with several unique topics related to BPM. International texting is also supported.

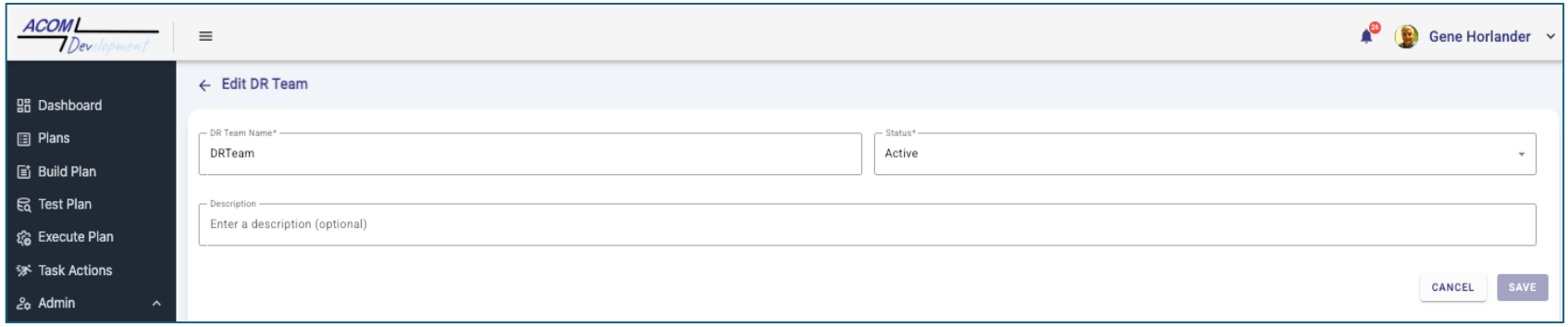


BPM Key Fields:

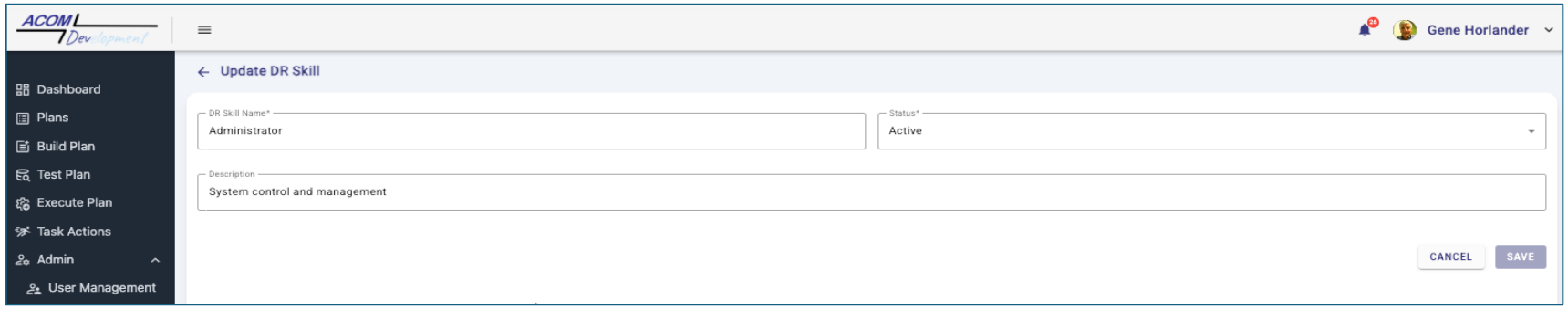
BPM provides the ability to add or edit key field entries via the administrative menu. Each key field has corresponding menu selection that will guide the user through this process.

A convenient feature provided by BPM is the ability to use shortcuts during the build process. Should a new field entry be required during the build process, rather than exit the build process, create the new field, then restart the build. Users can click on the "+" icon located to the right of a field. By clicking on the + icon, the corresponding entry creation functionality pops-up in the middle of the build process screen allowing the entry to be created, then returns to the build process.

DR Team name: You can create any number of teams, and then select team members to the DR team. You can use the default team name, going forward you may desire additional team assignments as workflows increase in complexity.



DR Skill: Defines the skill required for certain functions.



Roles:

Roles: Used to further refine a user's skills and capabilities within BPM. Select a role which is displayed in the forementioned permissions menu option. By default, you already have the administrator role which is the highest level. Other common roles are:

- **Team member**, role for a member of your DR Team
- **BR Manager** is for the team manager and will have access above the role of Team member.
- **BP Executive Director** is the only role authorized to declare a disaster.

The balance of the fields in the User's record relates to the user address, email, and phone number for text messages. BPM supports international text messaging.

Emergency contact information, address, and relationships to the user are required.

Default Settings:

- Acknowledge Time – the time period in minutes allowed to accept task, typically 15-minutes.
    - History/Log (system only)
- TBD
- TBD

Department:

Create/Edit /Delete departments:

- Title
- Department Code; 9 digits alphanumeric
- Status: Active / Inactive
- Description: 256 alphanumeric characters
- History/Log (system only)

Skills:

Create/Edit/Delete DR Skill

- DR Skill Name
- Status: Active / Inactive
- Description: 256 alphanumeric characters
- History/Log (system only)

Team:

Create/Edit/Delete DR Team

- DR Team Name
- Status: Active / Inactive
- Description: 256 alphanumeric characters
- History/Log (system only)

Plan Type:

Create/Edit/Delete DR Plan Type

- DR Plan Type Name
- Status: Active / Inactive
- Description: 256 alphanumeric characters
- History/Log (system only)

Site:

Create/Edit/Delete Site

- Site Name
- Site Code – 50 alphanumeric characters
- Street Address
- Country
- State
- City
- Zip code
- Status: Active / Inactive
- Description: 256 alphanumeric characters (optional)
- History/Log (system only)

Role:

Create/Edit/Delete Role

- Role Name
- Status: Active / Inactive
- BR Plan Permissions
- User
- Site
- Department
- System
- Plan Level
- Plan Type
- Other
- Default Configuration
- DR Skill
- DR Team
- System Type
- History/Log (system only)

Plan Level:

Create/Edit/Delete Plan Level

- Plan Level Name
- Status: Active / Inactive
- Description: 256 alphanumeric characters
- History/Log (system only)

System:

Create/Edit/Delete Plan Level

- System Name
- System Code: 9 alphanumeric characters
- Description: 256 alphanumeric characters
- Status: Active / Inactive
- History/Log (system only)

Pricing Model

Each license includes one advanced administrator license.

License can be mixed and matched to reduce cost.

To order online following this link https://www.acomdev.com/pricing , major credit cards accepted.

BPM Plans	# Team Members	# Sequences	# Task	# Plans	Monthly Fee
Personal	0-5	1	25	1	Free $0
Starter	10	2	50	2	$9.95/user/mo.
Professional	25	5	75	5	$19.95/user/mo.
Advanced	50	10	100	20	$49.95/user/mo.
Enterprise	Contact Sales				
Consulting/Training	40-hour package				$4,560.00

Appendix A – Security Statement

1.1 Organization

Enterprise Readiness Overview

Product/Service: BPM – Business Process Management v. 1.1.5
Company: ACOMdev, LLC
Document Version: v1.0
Last Updated: 2026.01.05
Primary Security Contact: Gene Horlander, ghorlander@acomdev.com
Support Contact: support@acomdev.com
Trust Center: Https://www.acomdev.com

Executive Summary

ACOMdev LLC provides software development and support. This document summarizes our security, privacy, and operational controls to support enterprise due diligence. Detailed evidence (policies, procedures, test summaries, and audit artifacts) is available under NDA upon request.

Key Commitments

- Data protection and privacy-by-design
- Secure software development lifecycle (SSDLC)
- Continuous monitoring and vulnerability management
- Incident response and disaster recovery preparedness
- Third-party and subprocess or risk management

Independent Assurance (Current Status)

- SOC 2: In Progress / Type I Complete / Type II WIP – 07.01.2026
- Penetration Test: 11/15/2025 — Summary available: Yes
- Vulnerability Scanning: Daily — Summary available: Yes
- ISO/IEC 27001: In Progress / Certified

Service Description and Scope

2.1 In-Scope Service

- **Service Type:** SaaS / PaaS / API / Mobile App / Desktop App / Hybrid
- **Environments:** Prod / Staging / Dev
- **Regions:** Global

Primary Use Cases:

- Corporation IT Management
- Data Center Management
- Health Service Management
- Hospital Process Management
- Cyber Response
- Disaster Recovery
- Business Continuity
- Policy / File / Military Search & Rescue

2.2 System Boundary (What's In / Out)

In Scope

- BPM core API
- Front-end graphics interface
- Mobile device interface and API (IOS and Android)
- Azure / AWS hosting model
- Customer Internal Cloud Hosting

Out of Scope

- Customer endpoint devices, customer-managed IAM, on-prem integrations

2.3 Data Classification and Handling

- **Customer Data Types:** PII, PHI, financial, IP, files, metadata, etc.
- **Data Sensitivity:** Low/Moderate/High or your internal scheme
- **Encryption:** In transit Yes, At rest Yes
- **Data Residency Options:** Yes – Automated dispatching

Architecture Overview

3.1 High-Level Architecture

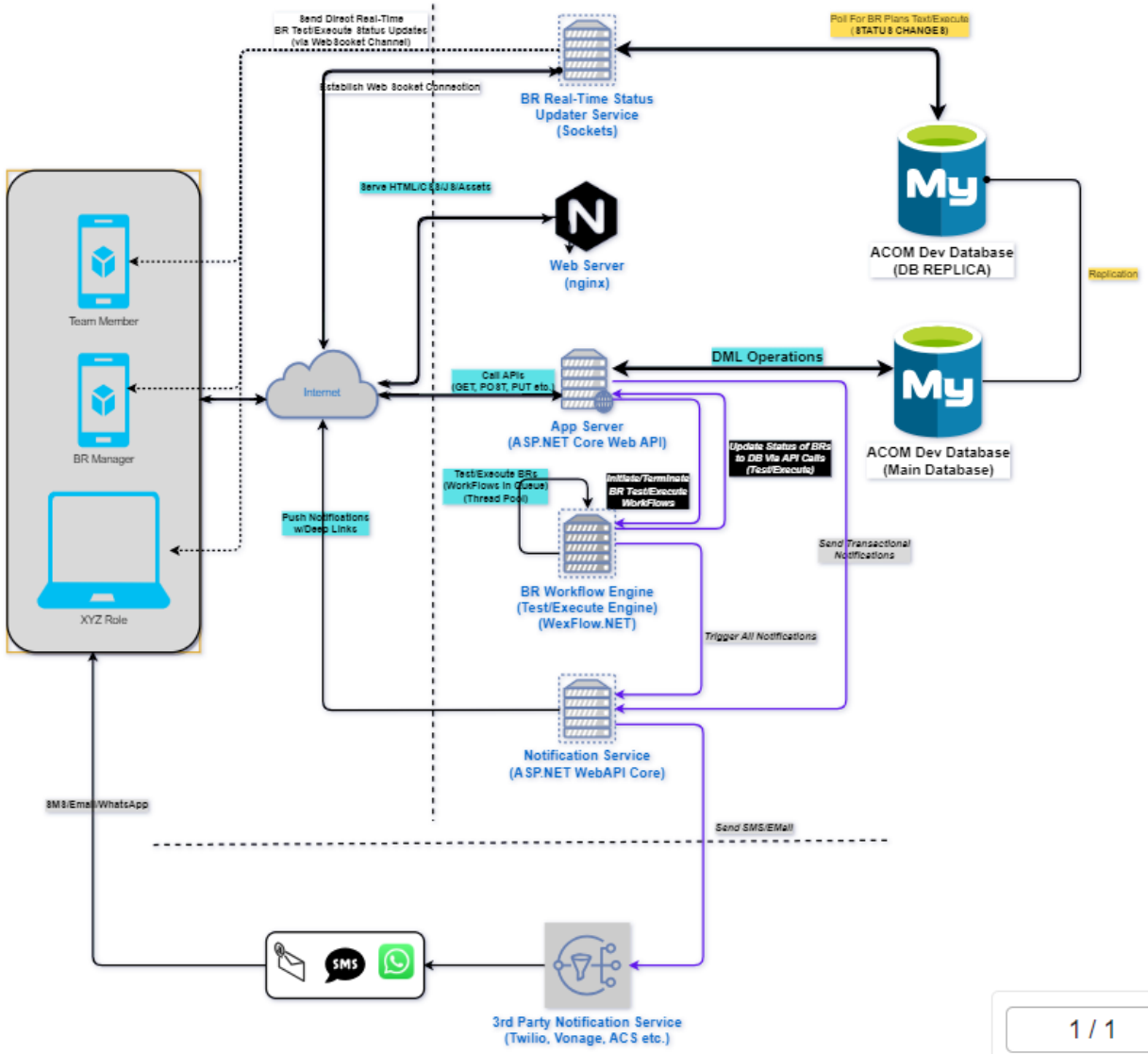
1) **Web Server** – ACOMDev website will be hosted on a web server running on NGINX
2) **App Server** – ACOMDev APIs will be hosted on the app server running on ASP.NET Core Engine

BR Status Updater Socket Server – Establishes Web Socket connections with client mobiles/browsers to send real-time status updates on BR Tests/Executions

BR Workflow Engine – A server that executes the Workflows associated with BR Tests & Executions

Notification Service – A server that encapsulates all notifications to the users – push notifications, SMS, Email, WhatsApp. For the later 3, a 3rd party service like, Twilio, Vonage, Azure Communication Services etc. will be used.

ACOMDev BR System Architecture Diagram



3.2 Key Components

Architecture

There are five services running and two DBs running in the backend, all internal communications between servers and clients are AES 256 bit encrypted.

Services

Following are the five services that will be running in the backend,

Web Server – ACOMDev website will be hosted on a web server running on NGINX

App Server – ACOMDev APIs will be hosted on the app server running on ASP.NET Core Engine

BR Status Updater Socket Server – Establishes Web Socket connections with client mobiles/browsers to send real-time status updates on BR Tests/Executions

BR Workflow Engine – A server that executes the Workflows associated with BR Tests & Executions

Notification Service – A server that encapsulates all notifications to the users – push notifications, SMS, Email, WhatsApp. 3rd party services like Twilio, Vonage, Azure Communication Services etc. are also used.

User Authentication – provides 2FA

Database

The Source DB of all schema and data will reside in a MySQL DB via encrypted portals.

A Replica DB of all schema and data will be available and is read-only DB. It will be used for,

Primarily for the Workflow engine and the Real-Time Status Updater Service to fetch status details of BR Tests & Executions. This will be high throughput fetch operations and hence they connect to replica, thus offloading these requests from the source DB

For high availability in production setup

Front End

The Front End uses Ionic w/Angular w/Capacitor w/AppFlow.

Ionic w/Angular ensures easy development & deployment of one codebase to all platforms – web, Android, iOS

Ionic w/Capacitor provides access to native modules like network, storage, mic, camera etc. as required + ability to use/create custom plugins for various needs

Ionic w/AppFlow (https://ionic.io/appflow) provides a unified set of tools for building and deploying apps to Android & iOS. It provides integration with GitHub in its CI/CD pipelines. All communications are encrypted.

3.3 Dependencies and Sub processors

A full list is available on request. Common categories:

- Cloud hosting: typically, Azure or AWS, customer dependent
- Monitoring/logging: Zabbix
- Support/ticketing: HDPlus/HubSpot
- Email/SMS: Microsoft
- Analytics: Microsoft Power BI

Security Governance

4.1 Policies and Program

We maintain and review security policies covering:

Access control, acceptable use, and password/MFA standards

Secure development and change management

Incident response

Vulnerability management

Business continuity and disaster recovery

Vendor risk management

Policy Review Frequency: Semiannual

Security Training: annual, includes phishing / secure coding / privacy

Roles and Accountability

Security Owner: Gene Horlander, CEO

Engineering Owner: Charles Boone, SR. Admin

Privacy Owner (if separate): Gene Horlander, CEO

Compliance Owner: Jamie Man, Security Admin

Identity and Access Management

5.1 Internal Access Controls

SSO: Yes – Provider: Azure AD

MFA enforced: Yes

Least privilege / RBAC: Yes

Access reviews: Monthly

Privileged access management: Microsoft Entra

Customer Access

6.1 Customer Access Controls

Authentication methods: SAML/OIDC

Audit logs available to customers: Yes – Retention: 365 days

Role-based access: Admin and Users

Data Protection and Cryptography

6.2 Data Protection Controls

Encryption in Transit: TLS 1.2+ / TLS 1.3

Encryption at Rest: AES-256 / cloud-managed keys / customer-managed keys option

Key Management: KMS/HSM, rotation: Monthly

Secrets Management: Vault/KMS/secret store, no secrets in code: Yes

Data Segregation: Logical tenant isolation / per-tenant keys / separate DB schemas

Secure SDLC and Change Management

7.1 SDLC Controls

Code reviews required: Yes

Branch protections: Yes

CI/CD approvals: Yes

Artifact integrity/signing: Yes – Method: Cosign, downloaded with audit trails

Release process: both standard and emergency require change control approval

7.2 Security Testing

SAST: GitHub CodeQL, frequency: continuously

Dependency scanning: GitHub CodeQL, frequency: continuously

Secrets scanning: GitHub Secret Scanning, frequency: continuously DAST: GitHub, frequency: continuously

Container/IaC scanning (if applicable): GitHub, frequency: all uploads and downloads are first scanned

SBOM: [Provided on request]

7.3 Vulnerability Remediation SLAs

Severity	Target Remediation Time
Critical	Immediately
High	24-hours
Medium	2-days
Low	1 week

Logging, Monitoring, and Auditability

8.1 Security Logging

Centralized logging: Yes

Security monitoring/alerting: Yes – Tooling: Bitdefender

Time sync: NTP enforced

Log retention: 30 days, then monthly

Customer audit logs: Yes – Export: API and CSV

Incident Response

9.1 Program Overview

We maintain an incident response plan that includes:

Triage and severity classification

Containment, eradication, recovery

Root cause analysis and post-incident review

Customer communications and timelines

Evidence preservation

9.2 Customer Notification

Notification trigger: confirmed incident impacting customer data/service

Initial notification: within 4 hours of confirmation

Updates cadence e.g., daily or as material changes occur

Post-incident report: within 3 days

Business Continuity and Disaster Recovery

10.1 Business Continuity and Disaster Recovery

Backups: Daily, encryption: Yes

Restore testing restores tested monthly

RPO: 4 hours

RTO: 4 hours

High availability: only mission critical systems, details: automated failover

Status page: Https//: www.acomdev.com\status

Privacy and Compliance

11.1 Privacy Practices

Data minimization: Yes

Purpose limitation: Yes

Access to customer data: Restricted and logged

Data deletion: requires change control and backup

DPIAs (if applicable): Yes

11.2 Regulatory/Framework Alignment

We align our program with recognized frameworks and customer expectations, including:

SOC 2 Trust Services Criteria: Security + optional criteria

ISO/IEC 27001: ISMS scope

NIST 800-53/FedRAMP: **Alignment with Roadmap**

Third-Party Risk Management

12.1 Risk Management

Vendor onboarding security review: Yes

Sub processor contract requirements: NDA, confidentiality, security controls, and breach notification

Annual vendor review cadence: Yes – Vendor scorecard approach

Critical vendor list maintained: Yes

Customer Security Responsibilities:

Managing user provisioning and access permissions

Enforcing customer-side MFA/SSO

Securing endpoints and browsers

Configuring integrations and API keys securely

Reviewing audit logs and alerts (if enabled)

Evidence Index (Available Under NDA)

Evidence Item	Description	Availability
SOC 2 Report	Type I/II	[NDA required]
ISO 27001 Certificate	Scope + certificate	[NDA/public]
Pen Test Summary	Exec summary + remediation status	[NDA required]
Policies	Security, IR, BCDR, Access, SDLC	[NDA required]
Architecture Diagram	High-level	[NDA/public]
Vulnerability Mgmt Metrics	SLA compliance snapshot	[NDA required]
Sub processor List	Vendor list + purpose	[NDA/public]