HEAT - PIR

New User Guide

Quality Assurance
July 2012

Table of Contents

Table of Contents 2
Revision History 3
PIR Submission Guidelines 4
When Should a PIR be Submitted? 4
PHI (Personal Health Information) 4
Critical Systems 5
What is Gold Code? 5
Severity 6
Business Impact 8
Creating a New PIR 10
Status Update Guidelines 17
Status Update Process 18
Sending Status Updates 19
Resolving a PIR 24
Closing a PIR 26
Changing Ownership 27
Customer Impact Details 28
What if I need Help? 30

Revision History

Edited by	Date	Reason for Change
Sheri Anderson	10/17/11	Formatting updates
Sheri Anderson	02/14/12	- Updated Contact Info - Removed "Quick Tips" - Updated Critical Systems List - Formatting updates
Sheri Anderson	05/31/12	- Updated verbiage on 15 minute submission rule - Updated Severity Criteria for SL3 - Modified New PIR steps to Save prior to sending email notification - Added Matt McCurdy as Incident Manager contact for SL1 & SL2 - Updated Assignment Group info for SL1 & SL2 - Updated use of Resolution Type for new PIRs - Added values to Critical Systems list - Added values to the Resolution Type - Added PHI fields - Modified Severity to include escalation process and PIR Incident Team - Removed escalation process from Business Impact section - Added step to SAVE the PIR prior to emailing notification - Added Service Desk info and causes for email notification issue - Removed HEAT specific training items - Added SharePoint link to Help section
Sheri Anderson	07/11/12	- Added Plan Connexion to the Critical Systems List

PIR Submission Guidelines

These guidelines should be used to ensure problems are reported quickly and the appropriate teams are working towards a resolution that is in line with the **Business Impact**, **Severity** and overall urgency of the problem.

A PIR should be submitted <u>within 15 minutes</u> of notification of the problem.

This applies to all Severity level PIRs. This is an important reminder as we need to provide impacted users enough time to prepare for workload impacts.

When Should a PIR be Submitted?

- Any single identified incident with a system/application on the **Critical Systems** list (see page 5)
- The **Severity** of one or more Service Desk calls is SL-1 or SL-2
- 10+ Service Desk calls are received for the same incident where there is no known resolution
- When an external system or process impacts BCBSAZ or impacts our customers
- The **Business Impact** of one or more Service Desk calls is High or Critical
- Anytime a new entry is created in the **Adjustment Rework** database and the new entry is not already associated with a PIR (*refer to* PIR - Adjustment Tracking Guidelines)
- When an incident impacts a major project milestone

PHI (Personal Health Information)

- **PHI** must never be keyed into any type of HEAT ticket on any tab or within any attachment
    - PHI includes, but is not necessarily limited to the following:
        - Subscriber ID
        - Member/Subscriber Name
        - Member/Subscriber Birth Date
        - Member/Subscriber Street Address
        - Member/Subscriber Phone Number
        - Member/Subscriber email Address

Critical Systems

- **Business Impact** and **Severity** values may be escalated for those on the Critical Systems list

- A PIR should be submitted for any single identified incident with a system/application on the **Critical Systems** list:

  - BizTalk
  - Business Ware 3 *
  - Business Ware 4 (Vitria) *
  - Clearinghouse (CCH)*
  - Claims Research Database (CRD) *
  - Common Financial
  - Corporate Data Warehouse (CDW)*
  - Customer Service Solution (CSS) – InfoMart Reporting *
  - Customer Service Solution (CSS) – Desktop *
  - Customer Service Solution (CSS) – Enterprise Routing Strategy (ERS) *
  - Doc1 (Billing, EOB/Remit, e2/Vault) *
  - Electronic Window *
  - eSales Web Application (Insurix/Connecture)
  - eChannel
  - FileNet *
  - Foresight
  - Genesys Voice Portal (GVP) *
  - Global 360
  - Image Retriever *
  - Internet (includes all portals) *
  - MetaVance/BIC
  - MetaVance Pricing & Configuration *
  - Plan Connexion
  - Pre-Adjudication Claims History (PACH)
  - TPS (Enrollment)

  **Gold Code certified*

What is Gold Code?

- The Gold Code strategy is to minimize the risk of disruption to business processes

- "Gold Code" is the production version of code for assets that BCBSAZ owns and supports

- The Gold Code Library is an indexing system used to make finding information easier; it references the assets, contacts and location of each Critical System as well as all application components and documentation that are required to rebuild and run the production system

- Using the Gold Code Library, IT will continuously perform Gold Code recovery tests to validate that we have all the components for each Critical System

Severity

- Information Technology and our customers will determine the Severity of a PIR based on ITIL (Information Technology Infrastructure Library) standard Severity levels

- The Severity will drive the escalation and notification process once a PIR has been submitted

- Criteria and examples should be considered carefully before selecting a value to ensure the PIR is addressed in an appropriate manner

- Contact the Incident Team (Nick Mendias, Matt McCurdy and/or the QATeam@azblue.com for assistance in creating and updating SL1 and SL2 PIRs – this team will assist until the PIR has been mitigated

SL 1 – Critical (Contact the Incident Team for creation and updates on these PIRs – until mitigation)	Criteria: • A critical production system is down and normal business processes cannot proceed • More than 90% of the users are affected • There is no timely workaround that provides the lost functionality • Severe business operation impact (Business Impact of 'Critical' or 'High') Examples: • Critical server failures that are core to business functions • Data corruption caused by software error or failure • Severe performance degradation, causing unreasonable waits for resources or response, or performance at a level that does not complete critical business functions
SL 2 – Urgent	Criteria: • A critical system is up, but not functioning at normal capacity • A major function is not available and it is affecting a significant number of users • Severe impact on business regardless of the environment • No acceptable workaround is available; however, business operations can continue in a restricted fashion • Severe impact to a single area Examples: • Severe performance degradation, causing moderate waits for resources or response • Critical system/application error or erroneous results caused by hardware or software error

SL 3 – High	Criteria: • Substantial Business Impact ('Medium' or above) or intermittent incident occurring in Critical System or application & customer-acceptable work around is available • Minimal degraded performance issue affecting Critical System or application • Substantial Business Impact ('Medium' or above) occurring in non-critical System or application where No acceptable work around is available Examples: • System supporting a critical application is down • Severe performance degradation, causing intermittent waits for response • Critical System or application erroneous results caused by hardware or software error
SL 4 – Medium	Criteria: • Serious Business Impact ('Medium' or above) or intermittent incident occurring in non- critical application • Work around is available and does not impact the majority of users • Minimal degraded performance issue affecting non-critical application or system Examples: • System supporting a critical application is down • Severe performance degradation, causing intermittent waits for resources or response • System/application error or erroneous results caused by hardware or software error
SL 5 - Low	Criteria: • Minor/negligible Business Impact ('Low') or intermittent incident occurring in non- critical application • Does not require an immediate sense of urgency – but is a task to be completed • Affecting a very low number of users • Is an internal request for reporting, not critical to business Examples: • Cosmetic issues • Re-spooling, printing or running of a report • Severe performance degradation, causing intermittent waits for resources or response • System/application error or erroneous results caused by hardware or software error

Business Impact

The following describes the criteria that must be met for selecting a Business Impact value:

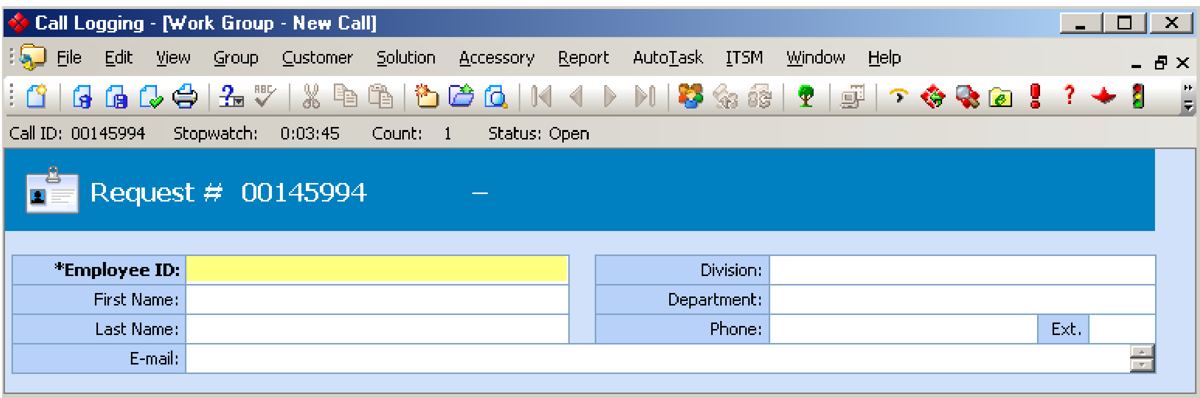
Low	Criteria • No significant business impact • May cause inconvenience, user is still able to complete task • Results in a condition not requiring immediate resolution Examples: • A desktop issue affecting a single user, user is still able to work • Cosmetic issue (misspelling, appearance of extra characters on screen) • Auto functionality not working, resulting in an extra step in process • Fields on screen are not highlighted according to message • Message does not appear on a report when not data is returned • Report truncating partial descriptions
Medium	Criteria • Moderate impact to business and/or customer service • Overall system and user effort can continue • A work around is available, may require additional effort • May cause slight increase in system suspense Examples: • Outage in <u>non</u>-critical application • Slowness or lag-time in system response • A desktop or network issue affecting < 20 users • Balancing issue with <u>non</u>-critical system screens or reporting

High	Criteria • Serious impact to business and/or customer service • No feasible work around • Overall system and user effort can continue • May cause low volume of payment errors • May cause significant increase in system suspense • Significant increase in customer service call volume Examples: • A desktop or network issue affecting a small number of users • Balancing issue with <u>critical</u> system screens or reporting • Batch job error preventing <u>non</u>-critical processing • Inaccurate claims, EOBs or ID cards exceeding 10% of daily volume • Outage in a <u>critical</u> **TEST** system/application
Critical	Criteria • Significant disruption to business and/or customer service • <u>Critical</u> system processing and user effort are halted • May cause high volume of payment errors Examples: • Outage in <u>critical</u> application or supporting system • Data corruption preventing processing in critical system/application • Batch job error preventing <u>critical</u> processing • Inaccurate claims, EOBs or ID cards exceeding 25% of daily volume

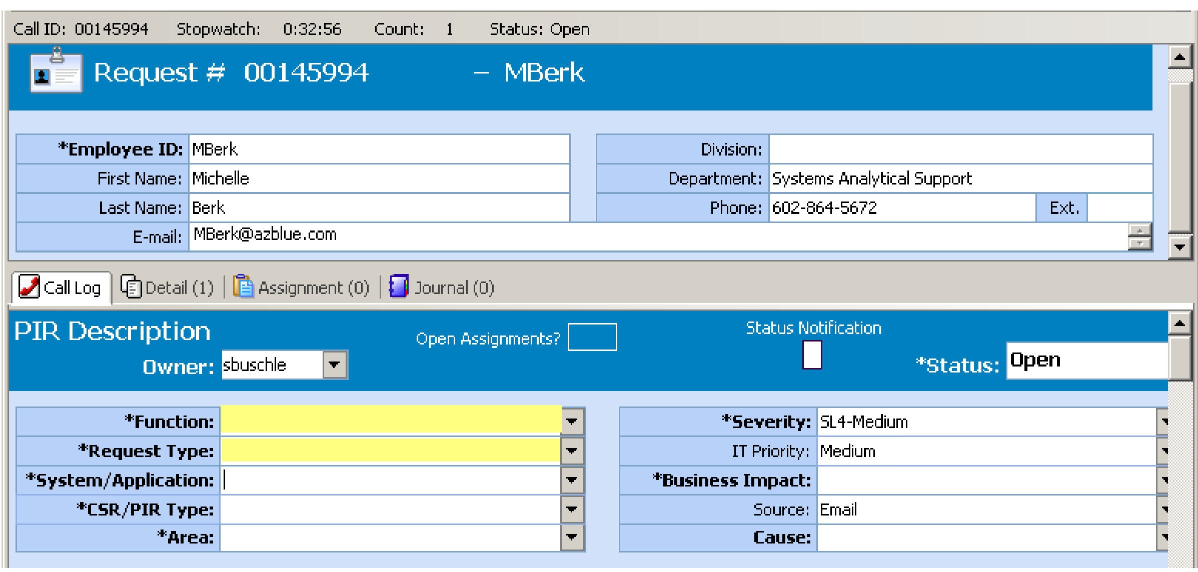
- If the analyst or team assigned to research/resolve the work item does not agree with the submitted Business Impact (based on the above definitions), they may change the value and notify the originator with an explanation

Creating a New PIR

1. Open a HEAT new ticket window
2. Use Login ID for the individual who <u>*identified*</u> the problem as the **Employee ID**
3. Hit the [tab] key to populate the remaining employee fields



4. **Function** → select 'PIR'
5. **Request Type** → select 'PIR'

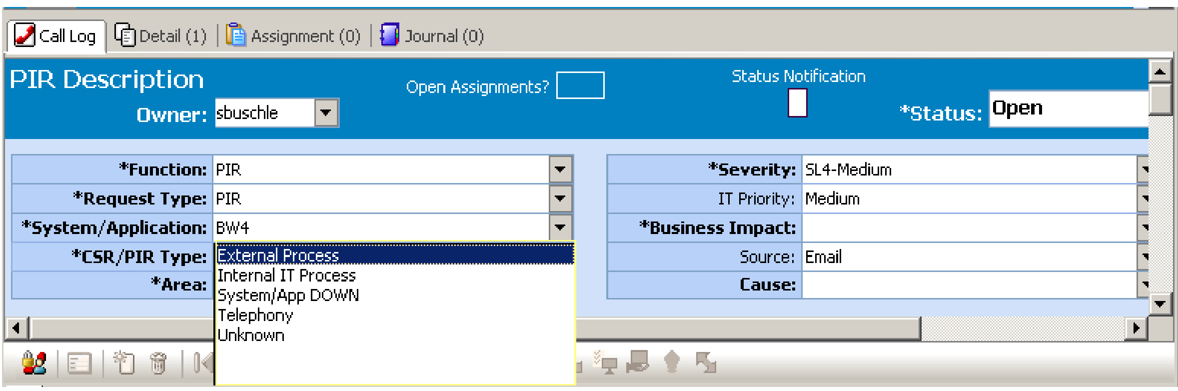


Please note: The **Owner** is responsible for all of the information and activity related to a PIR (see page 28 for additional details).

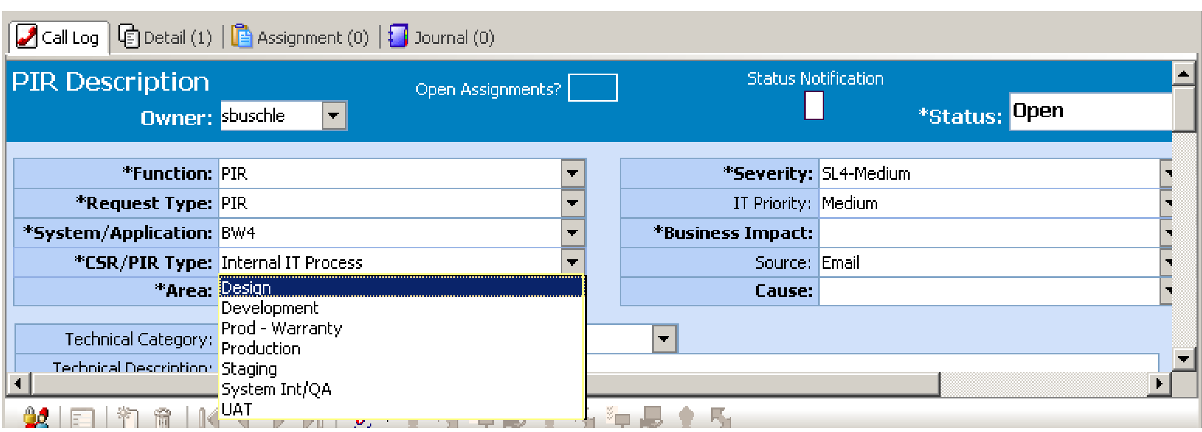
6. Change the **Status** to 'Analysis' prior to sending out any status update notifications (at the time the PIR is created, the default is 'Open' – see Status Values section on page 17 for additional information)

7. Select the applicable **System/Application** value

8. Select the **CSR/PIR Type** value



9. Select the **Area** where the problem was identified



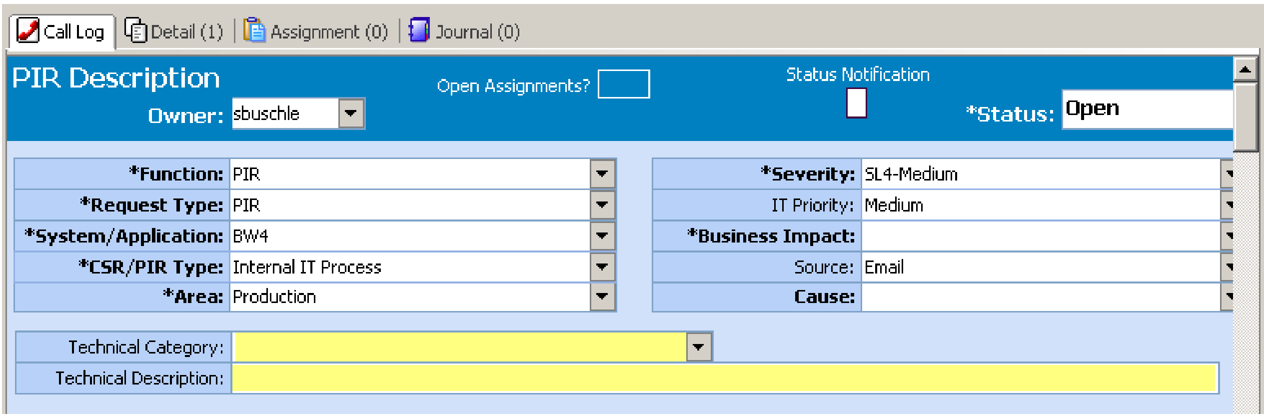
10. Select the appropriate **Severity** (default is 'SL4-Medium') based on ITIL guidelines

11. Select the appropriate **Business Impact**

12. Select the **Source** for how the problem was initially reported

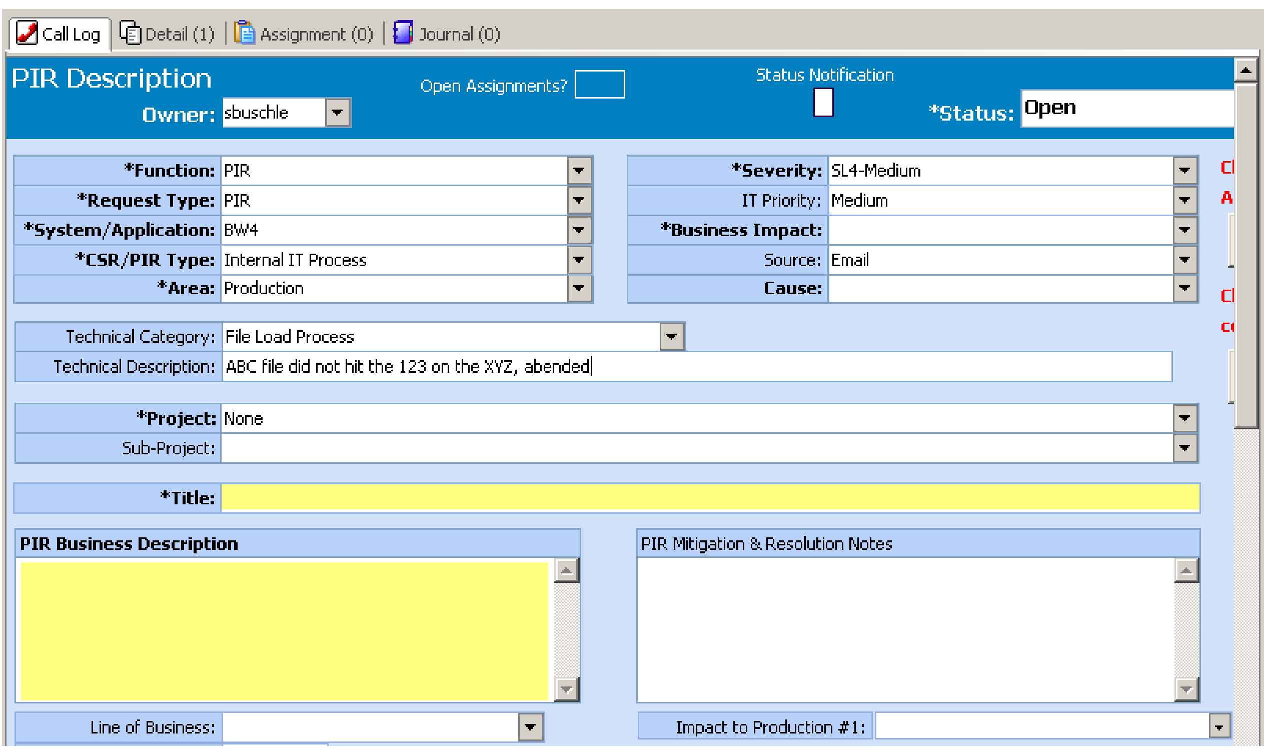
13. If applicable, select the **Technical Category** further defining the incident for the selected **System/Application**

14. Enter any applicable **Technical Description** notes (this can always be added to later)



15. Update the **Title** with a clear and concise summary of the problem

16. Enter a <u>non-technical</u> explanation and <u>impact</u> of the problem in the **PIR Business Description**



17. Add a non-technical explanation of actions taken, workaround, or other applicable comments to the **PIR Mitigation & Resolution Notes**

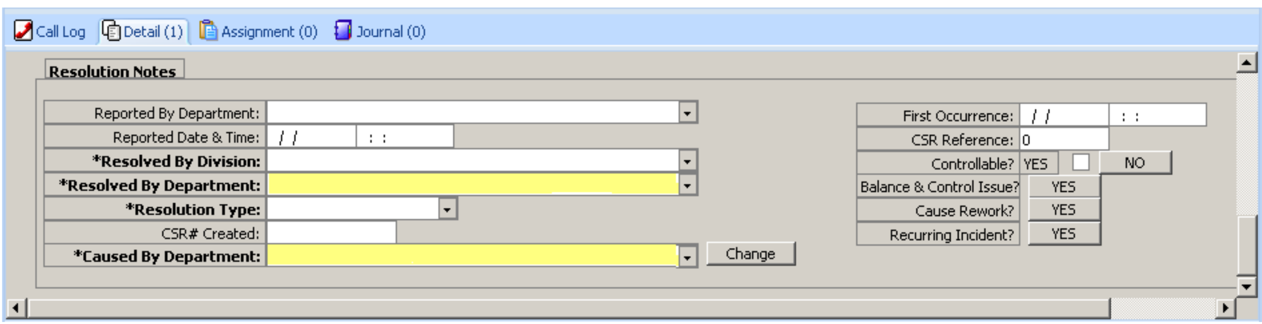
18. Click the Detail tab and scroll to the Resolution Notes section

19. Select a department from the ***Resolved by Department** field drop-down (*if unknown, select your own department)*

20. Select a department from the ***Caused By Department** field drop-down (*if unknown, select your own department)*

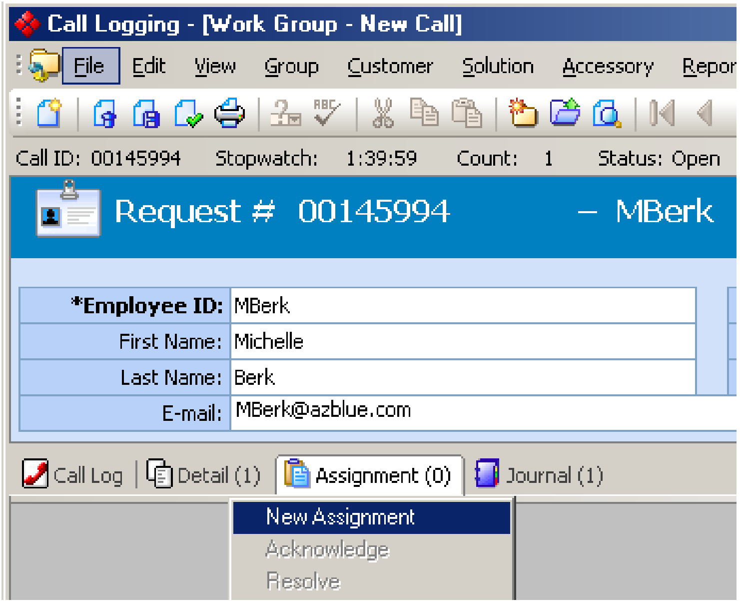
21. **If known,** select a ***Resolution Type**

   ***Resolution Type** is required at the point of mitigation. If it is **<u>not</u>** known when opening a new PIR, **leave the field blank**. Providing an inaccurate Resolution Type on a new PIR may be misleading.

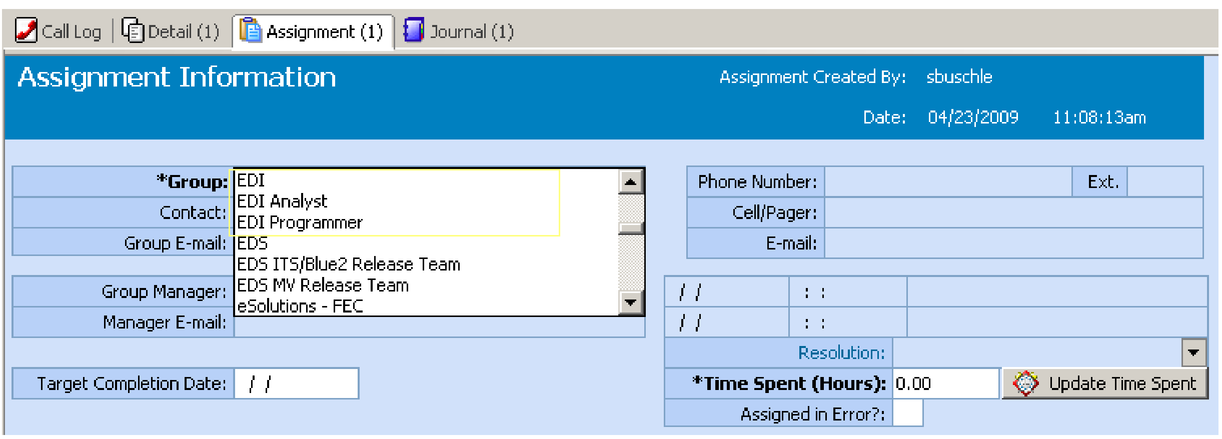


Please Note: *The Owner is responsible for updating the Resolved by Department and Caused By Department fields during the lifecycle of the PIR.*

Create a new **Assignment** by right-clicking on the Assignment tab

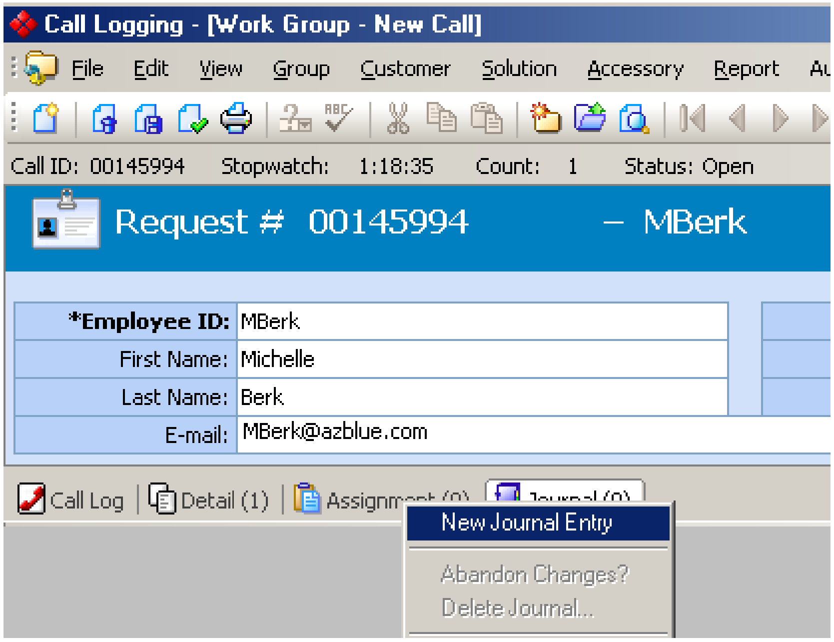


22. Select the **Group** for the area researching the problem



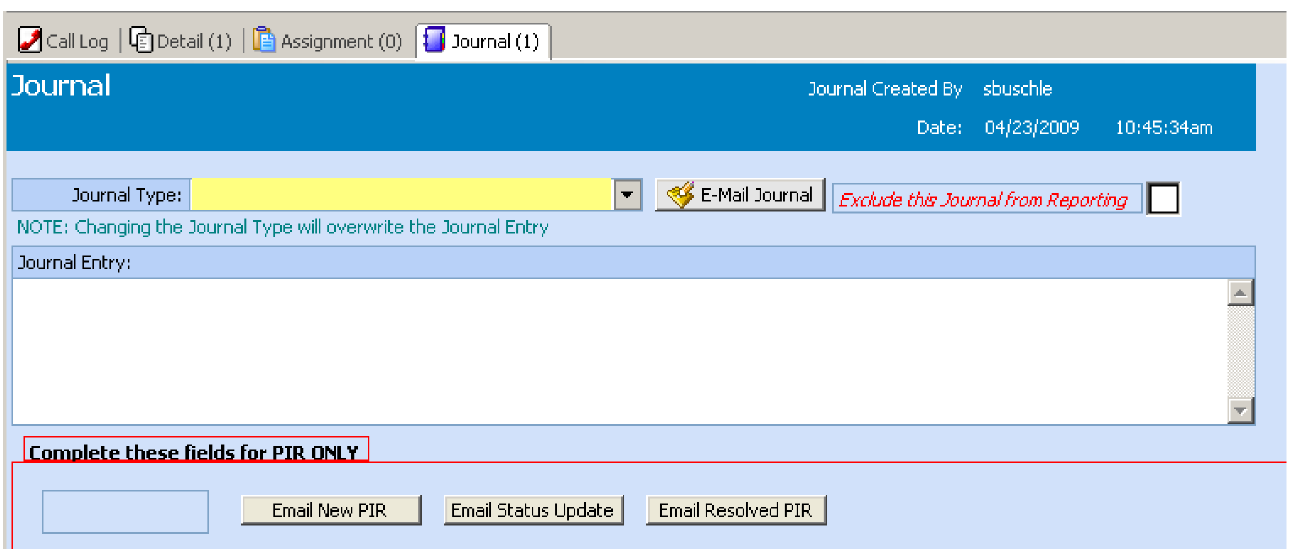
23. Create an additional Assignment to the **PIR – IT Incident Team** for **Severity** = SL1-Critical *or* SL2-Urgent

24. Create a new **Journal** entry by right-clicking on the Journal tab



25. In the **Journal Type** drop-down, key in 'PIR' and [tab] to see a list of PIR related values

26. Select 'PIR – Status Update' and click OK



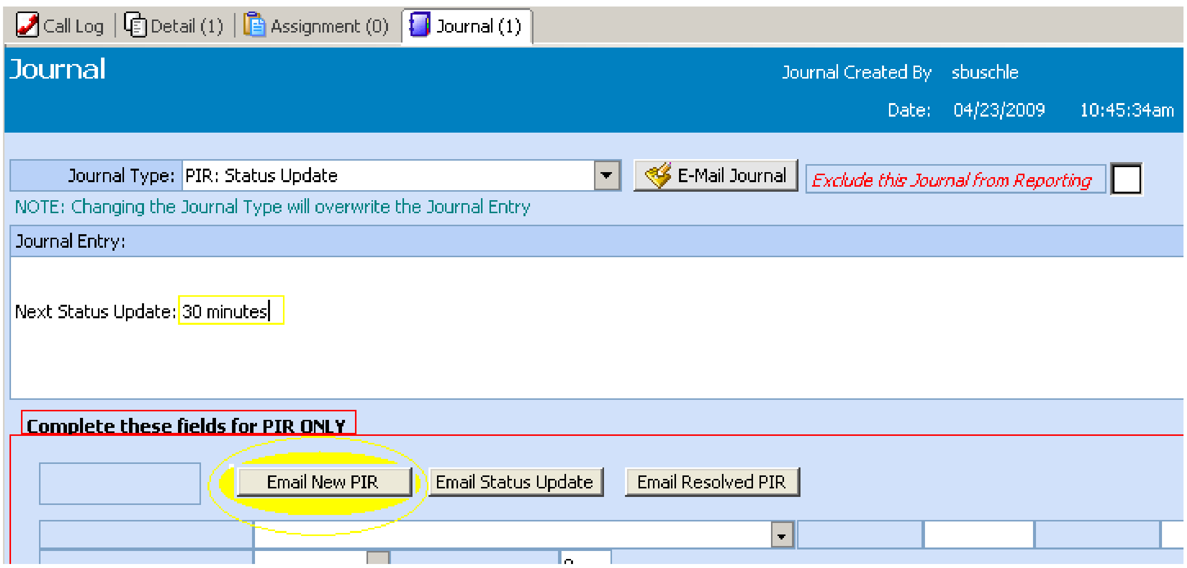
27. In the **Journal Entry** text field, describe activity or actions that are underway to research or mitigate the problem

28. Update the **Next Status Update** timeframe in the text box

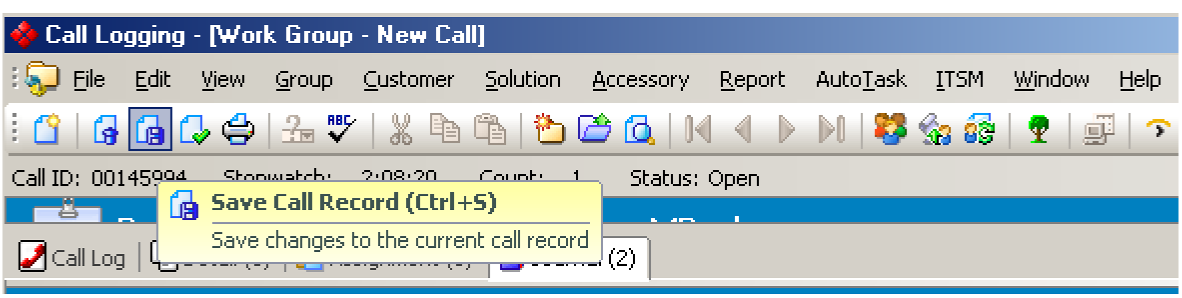
29. **Save** the Call Record!

30. Contact the Incident Manager (Nick Mendias or Matt McCurdy) on all SL 1 & SL 2 PIR's **before** the new PIR is emailed out to verify that the Severity level chosen is appropriate

31. Click **Email New PIR**



32. Save the Call Record!



The New PIR e-mail will be sent to the 'PIRProd' Outlook distribution group

If you click the e-mail PIR buttons and the e-mail does not go out as expected, please contact the Service Desk. One of the following is likely the cause:

- You have not attended PIR training, so you have not been granted the appropriate access to send the e-mail
- Your Outlook settings may need to be updated

Status Update Guidelines

These guidelines should be used to ensure problems are reported quickly and status updates are distributed on a schedule in line with the severity level and business impact.

How Often Should a Status Update be E-mailed?

It is the responsibility of the PIR **Owner** to create and distribute Status Update Journal entries.

- SL1 – Critical and SL2 – Urgent PIRs:
  - must be updated <u>at least every 30 minutes</u> for the first 90 minutes (original notification plus 3 status updates)
  - 90 minute update must specify the time the next update will be distributed
  - until mitigated, status update should be distributed as changes occur and/or no less than once per day
  - a status update should be distributed <u>any time</u> there is a significant information available (a cause identified, a work around put into place, additional business impacts are reported, a correction has been made)
- SL3 - High, SL4 – Medium PIRs:
  - Initial notification must specify the time the next update will be distributed
  - A 'PIR - Status Update' **Journal** should be distributed with any significant change in status, until mitigated
- SL5 – Low PIRs:
  - An e-mail notification is <u>not</u> required
  - These PIRs will be listed on the Daily Status Report

Status Update Process

Status Values

Status values are an integral part of the reporting process, so please update the values in a timely manner. These are the only values that should be used for PIRs, and they should always follow this order:

1. **Open** - the default Status for a new PIR

2. **Analysis** – initial notification has been distributed and a team has been assigned to research the incident and make an initial impact assessment

3. **Mitigated** – the severity of the incident has been reduced

   We will update the PIR Status to Mitigated for any of the following reasons:
   - a temporary workaround has been identified
   - the severity has been reduced, a resolution has been identified and the effort towards that resolution is in progress
   - a file fix has corrected the current situation and a permanent solution is being developed

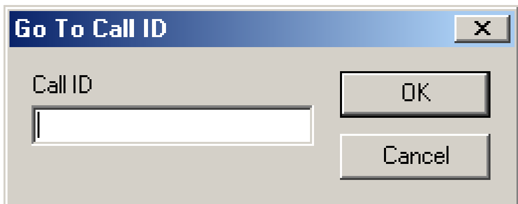
4. **Resolved** – determination to follow some course of action

   We will update the PIR Status to Resolved when all of the following conditions apply:
   - a permanent fix or workaround is moved into place
   - all research and work effort has been completed
   - a change (CSR) has been initiated
   - to allow time (14 business days) for gathering actual business impacts
   - to await completion of any business rework caused by the problem

5. **Closed** - all work related to the incident has been completed and documented in the PIR and all final business impacts have been documented in the PIR

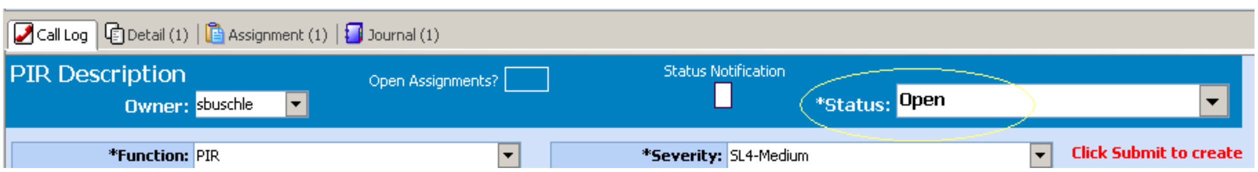
Sending Status Updates

1. From a HEAT ticket window, [ctrl-G] to Go To a call



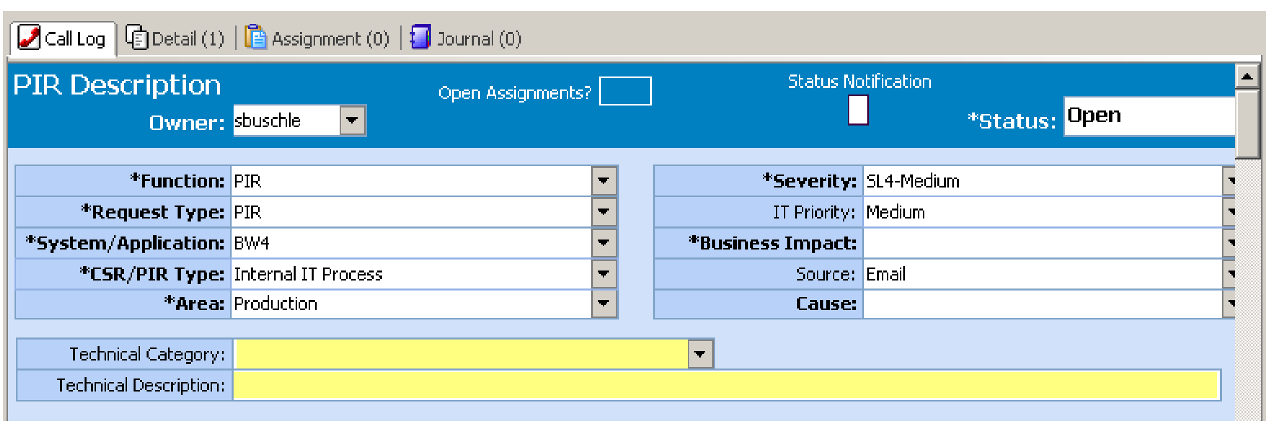
2. Enter the PIR Request #, click OK

3. Change the **Status** to the next appropriate status in the PIR lifecycle: Analysis or Mitigated



4. If missing, update the **Technical Category** further defining the problem for the specified **System/Application** (this data is used for PIR root cause analysis and service improvement)

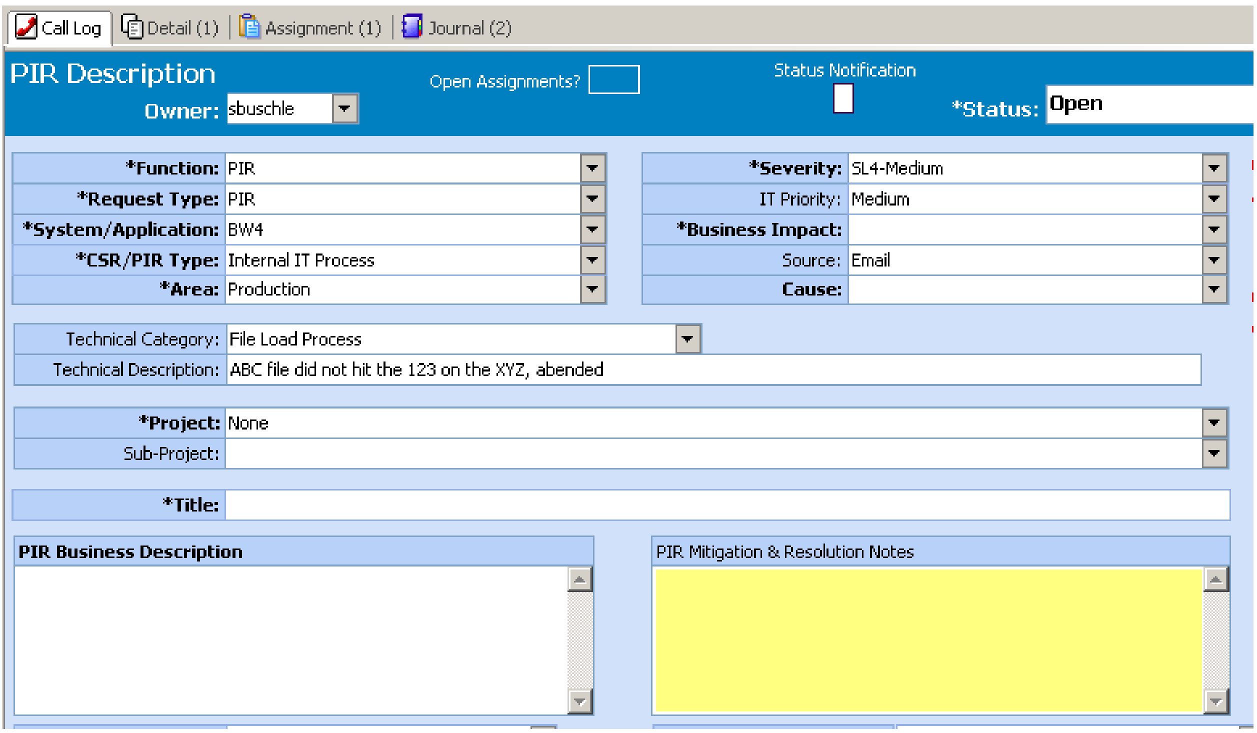
5. Enter any applicable **Technical Description** notes



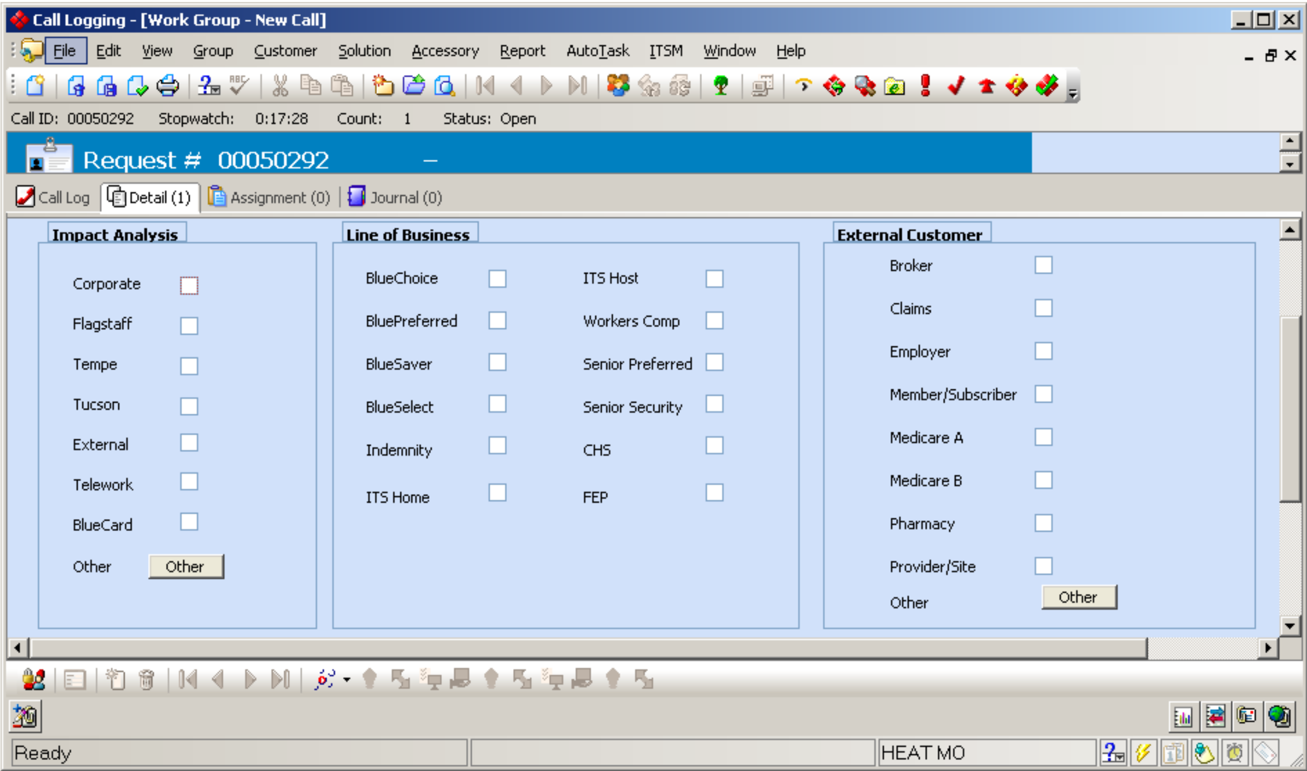
6. Update any new details and impacts with <u>non-technical</u> explanation of the problem in the **PIR Business Description** field

7. In the **PIR Mitigation & Resolution Notes** field, document steps taken to mitigate the problem using non-technical language (*this field may be updated, appended, or modified as needed during the life of the PIR*)

   - Were files reprocessed correctly?
   - Was a work around identified, if so what?
   - Was a CSR submitted, if so for what?
   - Is there anything else that may help customers understand the overall status?



8. Update any known values on the **Detail** tab



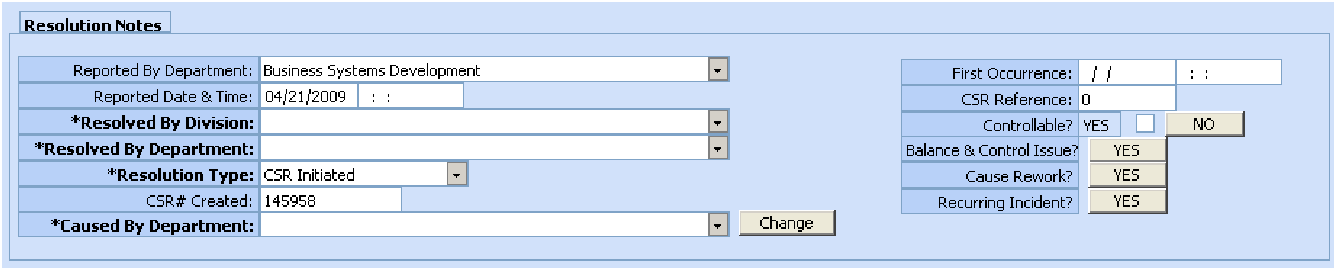
The center section of the Detail tab includes checkboxes for identified impacts.

- **Impact Analysis** – checkboxes represent the location(s) impacted by the problem; if an impacted location is not listed, the clicking the Other box will open a Journal to document the additional location

- **Line of Business** - checkboxes represent the line(s) of business impacted by the problem

- **External Customer** - checkboxes represent external customer types impacted by the problem; if an impacted type is not listed, the clicking the Other box will open a Journal to document the additional external customer type

9. Update the **Resolution Notes** section on the **Detail** tab



- **Reported By Department**
- **Reported By Date & Time**
- **Resolved By Division**
- **Resolved By Department** *(the Owner is responsible for updating this field during the lifecycle of the PIR)*
- **Resolution Type** (Back Out Update/Change CSR Initiated, File Reloaded, Hardware Replacement, Permanent Fix, Software Update, Temporary Fix, Workaround)

  NOTE: The **Resolution Type** field displays in the Subject line of the status e-mail, so be sure to select the appropriate value as soon as the issue has been MITIGATED

- **CSR # Created** (new Request # if a CSR was initiated as part of the resolution)
- **Caused By Department** (department primarily responsible for the problem - *the Owner is responsible for updating this field during the lifecycle of the PIR)*

  NOTE: The **Caused By Department** is used in a significant number of reports. If the department selected is incorrect, use the 'Change' button to clear the field before selecting a new department. When the 'Change' button is clicked, a Journal form will open. Please document the reason for the change in the text box.

- **First Occurrence** data and time (if known)
- **CSR Reference** (if a Request # is available for the first occurrence)
- **Controllable** (yes, if problem was within BCBSAZ control, no to document reason)
- **Cause Rework** (yes, if problem caused rework effort)
- **Recurring Incident** (yes, if problem is related to one or more previous incident)

10. Create a new **Journal** entry by right-clicking on the Journal tab

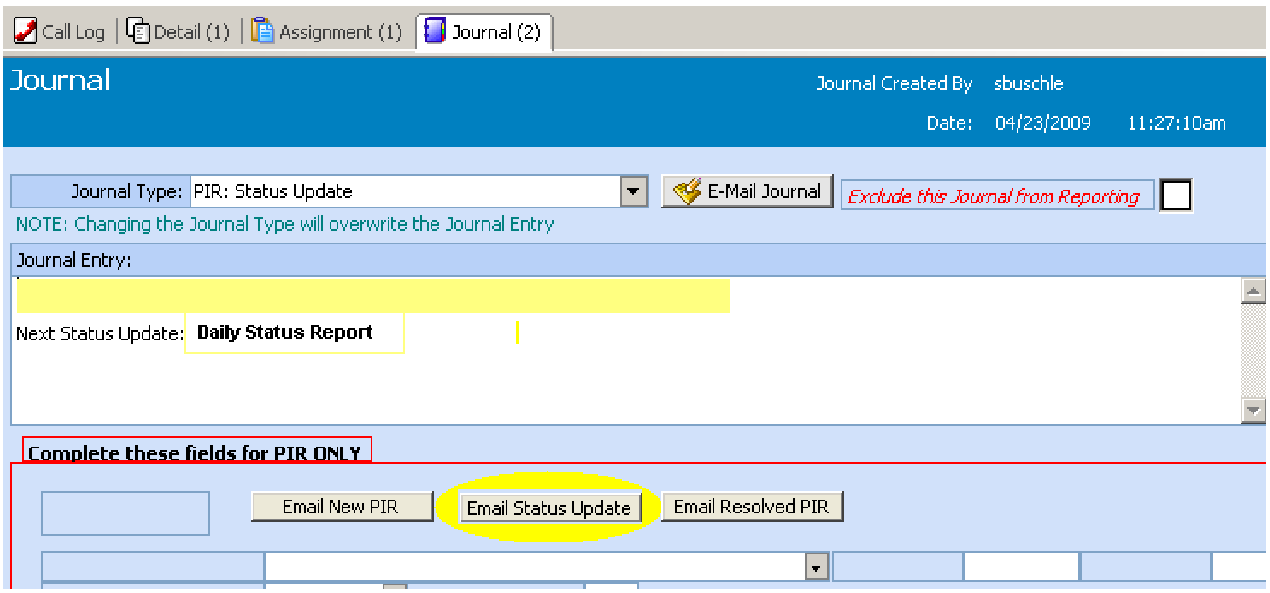
11. In the **Journal Type** drop-down, key in 'PIR' and [tab] to see a list of PIR related values

12. Select 'PIR – Status Update' and click OK

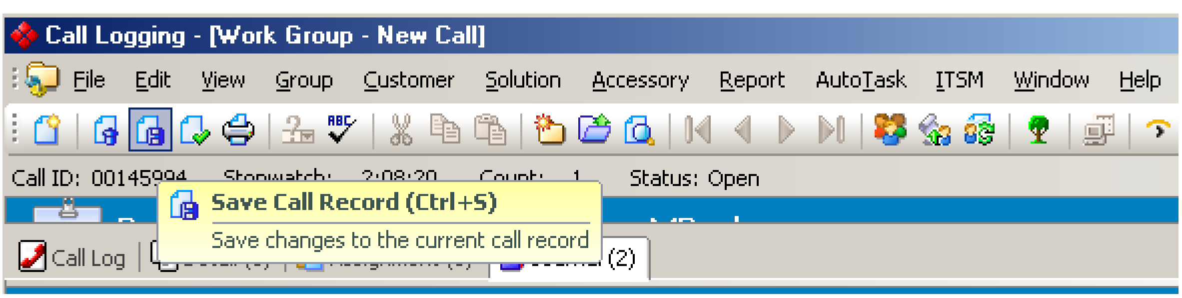
13. In the **Journal Entry** text field and using non-technical language, describe new activity or actions that are underway to research or mitigate the problem (*please do not report "no update"*)

14. Update the **Next Status Update** timeframe in the text box (default is '30 minutes')

15. Click **Email Status Update**



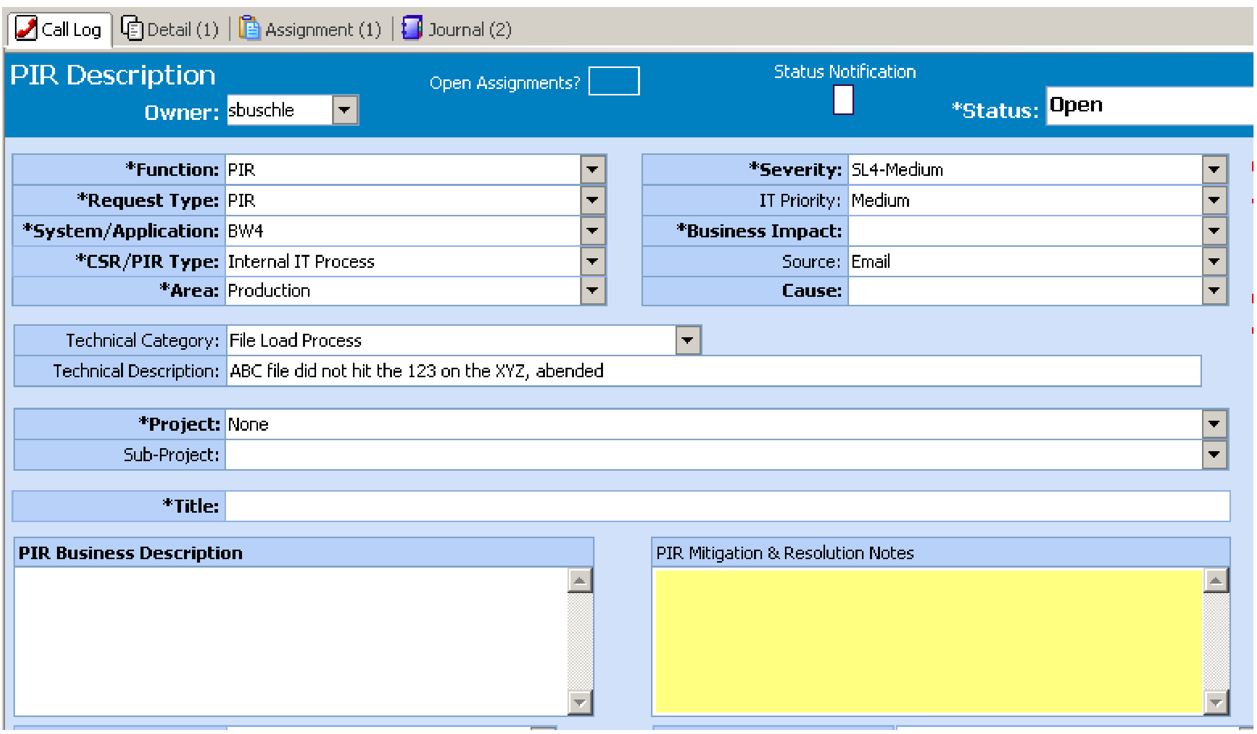
16. Save the Call Record!



Resolving a PIR

1. In the **PIR Mitigation & Resolution Notes** field, document the <u>root cause</u> of the incident

   - What was ultimately the cause of the incident?
   - What was done to prevent the same incident from occurring in the future?
   - Where there any balance & control procedures implemented to reduce the likelihood of a recurrence?
   - Where there any process changes implemented to reduce the likelihood of a recurrence?



2. Create a new **Journal** entry by right-clicking on the Journal tab

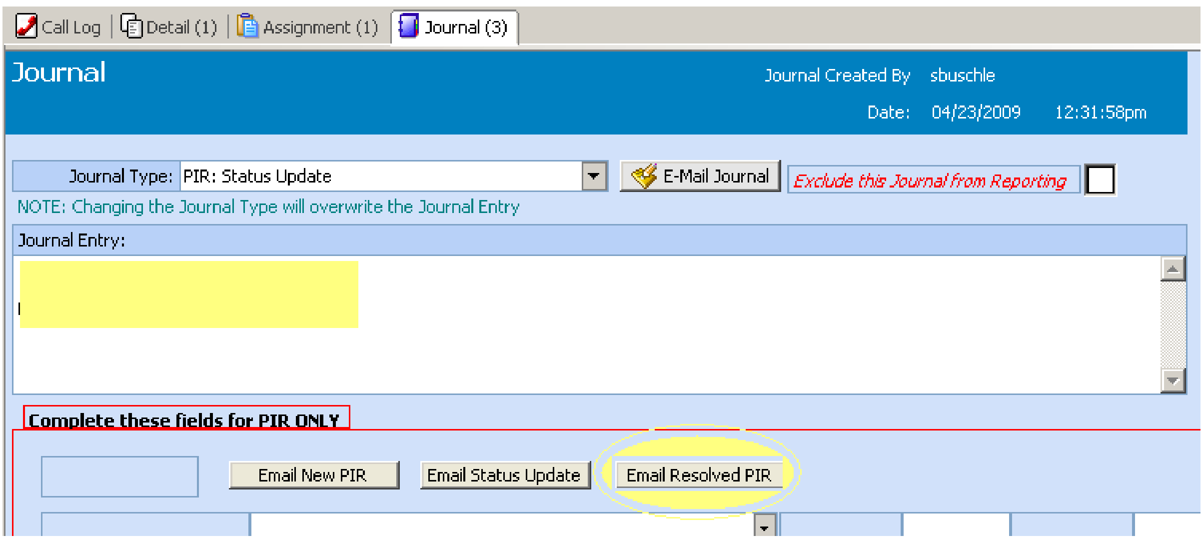
3. In the **Journal Type** drop-down, key in 'PIR' and [tab] to see a list of PIR related values

4. Select 'PIR – Status Update' and click OK

5. In the **Journal Entry** text field and using non-technical language, describe overall resolution to the problem (*these notes may be copied from the updated PIR Mitigation & Resolution Notes section)*

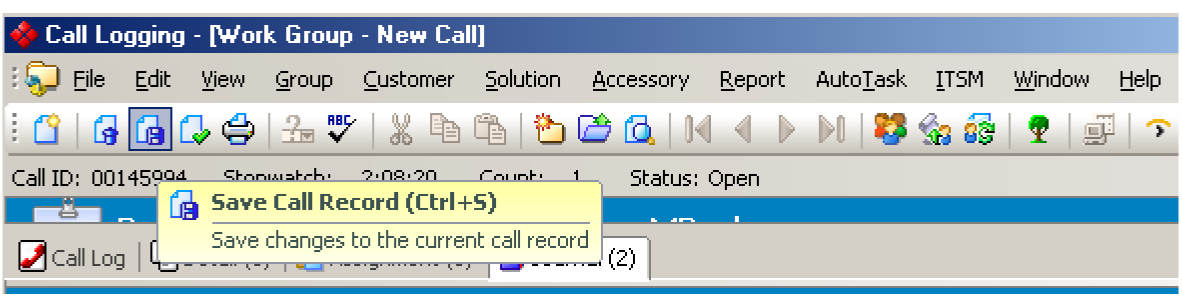
6. Remove the **Next Status Update** line from the text box

7. Click **Email Resolved PIR**



8. Close all open assignments and update time spent on analysis and research

9. Save the Call Record!



Closing a PIR

1. Ensure customers have had <u>14 business days</u> since the **Status** was changed to Resolved to update 'PIR: Customer Impact (Details)' Journal entries

2. Select the appropriate Call Log **Cause** value:

    - Change Management (any type of human error)
    - Software
    - Infrastructure (hardware, network, servers…)
    - Telecom
    - External

3. Change the **Status** from 'Resolved' to 'Closed'

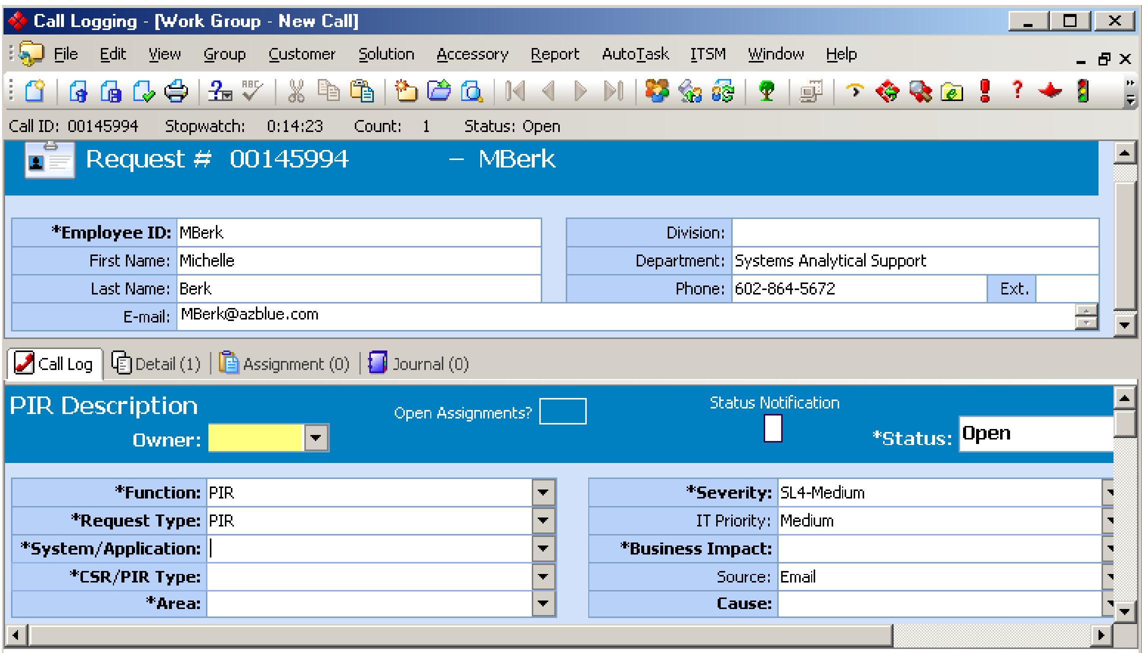
Please <u>do not reopen</u> a PIR if a problem reoccurs. Instead, create a new PIR and reference the original ticket.

Changing Ownership

The **Owner** is responsible for all of the information and activity related to a PIR.

At the time the PIR is submitted, the **Owner** will default to the employee creating the ticket.

If another person assumes responsibility for the PIR, the *new* **Owner** should change the value. This process will ensure the person assuming ownership is aware of the change in responsibility.



To change the value in the Owner field, the new Owner will:

1. Highlight and delete the existing value
2. Key in the first letter of his/her Network ID and click [TAB] to display the list of Owner values
3. Highlight the appropriate ID in the list
4. Click OK

Customer Impact Details

The PIR function accommodates gathering customer impacts of a problem from the time a ticket is created until the PIR is closed. Data will be used for root cause analysis in an effort improve overall service.

- Initial customer impacts should be entered as soon as the impact has been identified

- **Final customer impact details must be entered within 14 days of the 'Resolved PIR' notification e-mail**

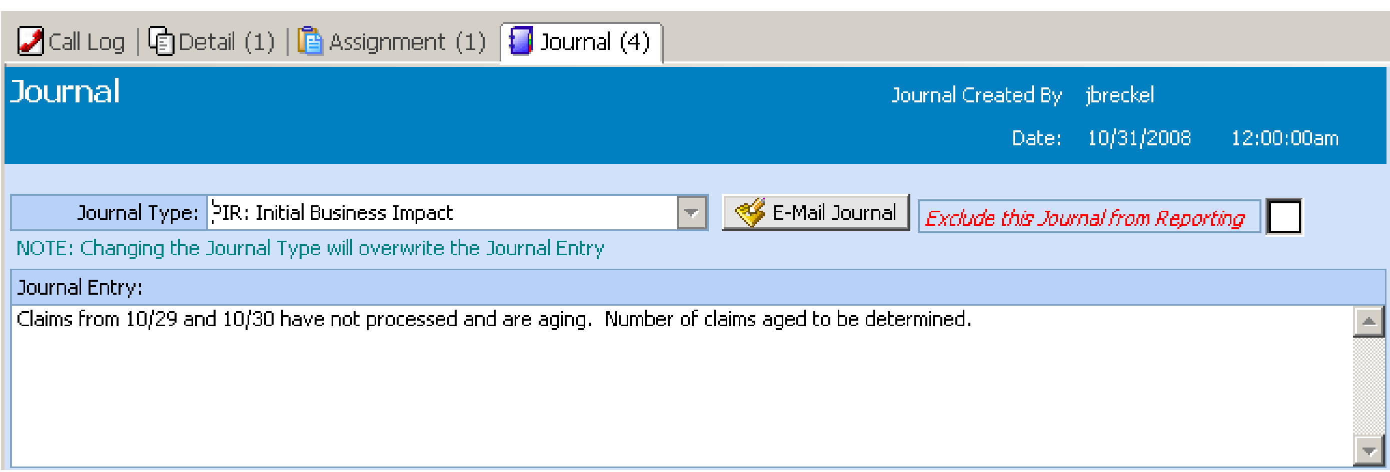
Initial Impact Updates

Business areas (Claims, Enrollment, FEP, etc.) are responsible for validating and/or updating the following information:

1. Values in the *Call Log* tab **Impact to Production #1-3** drop-downs. Values include:
   - Application Down
   - Causes Suspense
   - Incorrect Payment
   - Increased ACHT
   - Increased Calls
   - Lost Functionality
   - No Incoming Calls
   - Phones Down
   - Rework
   - System Down
   - Timeliness

2. Values for primary **Line of Business**, and primary **Metric Affected**

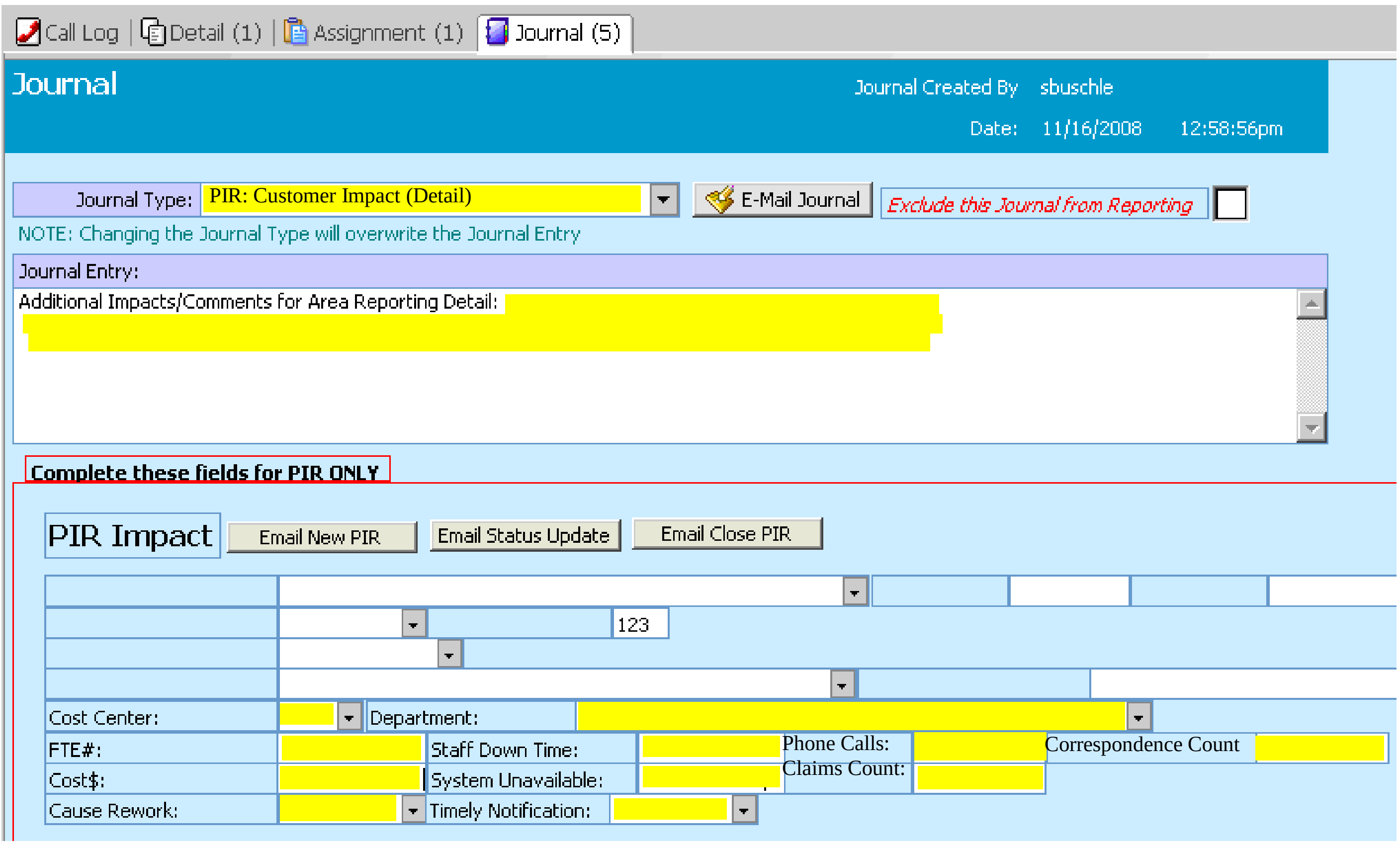
3. **Journal** entry for '**PIR: Initial Business Impact**'



Final Impact Updates

<u>At the time a PIR is moved to a Resolved Status</u> and before it is Closed, **EACH** area impacted is responsible for Creating a *Journal* documenting impacts specific to their area.

Creating a Journal (fields to be updated by business area are high-lighted)



1. With the PIR ticket open, click the *Journal* tab, right-click and select 'New Journal Entry'
2. Create a new *Journal* entry with a **Journal Type** of '**PIR: Customer Impact (Detail)**'
3. Choose **Cost Center OR Report Level Department** name
4. Document overall impact on the area in the **Journal Entry** text box
5. Enter applicable details for:
   - **FTE#**
   - **Cost$**
   - **Staff Downtime (Hrs)**
   - **System Unavailable (Hrs)**
   - **Phone Calls** (count related calls)
   - **Claims Count**
   - **Correspondence Count**
   - **Cause Rework** (Yes/No)
6. Click File → Save Call Record

What if I need Help?

Online Resources

- Check out the CCSA & QA SharePoint site for all current documentation: http://it.azblue.com/Departments/ccsa_qa/default.aspx

Quality Assurance

If you have questions related to PIR submission, please contact anyone on the Quality Assurance team or send an e-mail to QATeam@azblue.com.

- Sheri Anderson (602) 864-5794 *or* (623) 551-1712
- Teisha Bruyn (602) 916-7829
- Rebecca Thompson – reporting (602) 916-7738
- Tara Maya (602) 864-4066 *or* (623) 399-2377

PIR Training

To request PIR Training, please send an e-mail to QATeam@azblue.com.

Reporting

Submit report requests for PIR HEAT data as a HEAT DSS Reports CSR

PIR Updates

Valid values for drop-downs can be requested as a HEAT CSR assigned to the HEAT/QA Assignment Group

IT Service Desk

Contact the IT Service Desk (602) 864-4099 for any issues related to connectivity, application problems or security. Items that need to go through the Service Desk include:

- E-mails are not going out as expected
- E-mails are not received as expected
- SQL connection errors
- Screen display, keyboard or other issue that is unique to the desktop
- Name changes or issues with Employee displaying correct data

UAR Submission is required for:

- Access to HEAT or to change existing security role within HEAT
- Addition or deletion from the 'PIRProd' Outlook distribution group