

**Richtlinie:
Emergency Change (E-Change)**

Enterprise Core Services

der

BARMER und der HEK

Definition Emergency Change (E-Change)

Ein Emergency Change ist eine Änderung, die so schnell wie möglich implementiert werden muss. Diese Art von Änderung wird in der Regel durchgeführt, um kritische Vorfälle zu beheben oder Sicherheitslücken zu schließen.

Zu einem E-Change liegt meist ein Incident Priorität 1 (Service Ausfall) oder 2 (Drohender Service Ausfall) zu Grunde. Aufgrund der Dringlichkeit wird der normale Change Prozess beschleunigt.

Gründe für einen E-Change

- **Behebung kritischer Vorfälle:** Wenn ein schwerwiegender Vorfall auftritt, der den Betrieb erheblich beeinträchtigt, muss schnell gehandelt werden, um den Service wiederherzustellen.
- **Sicherheitslücken schließen:** Bei der Entdeckung von Sicherheitslücken, die ein hohes Risiko darstellen, ist eine sofortige Änderung erforderlich, um das System zu schützen.
- **Minimierung von Ausfallzeiten:** Durch schnelle Reaktionen auf Probleme können längere Ausfallzeiten und deren negative Auswirkungen auf das Geschäft vermieden werden.
- **Erfüllung gesetzlicher Anforderungen:** Manchmal erfordern gesetzliche oder regulatorische Änderungen eine sofortige Anpassung der Systeme.
- **Erhalt der Servicequalität:** Durch die schnelle Reaktion auf Vorfälle kann die Qualität und Verfügbarkeit der IT-Services aufrechterhalten werden.

Risiko

- **Erhöhtes Risiko:** Da E-Changes schnell implementiert werden müssen, bleibt oft wenig Zeit für umfassende Tests. Dies kann zu unerwarteten Problemen oder Fehlern führen.
- **Mangelnde Dokumentation:** Die Dringlichkeit kann dazu führen, dass Änderungen nicht ausreichend dokumentiert werden, was zukünftige Wartungsarbeiten erschwert.
- **Ressourcenbelastung:** E-Changes erfordern oft sofortige Aufmerksamkeit und können andere geplante Arbeiten unterbrechen, was zu einer ineffizienten Nutzung der Ressourcen führt.
- **Potenzielle Instabilität:** Schnell implementierte Änderungen können die Stabilität des Systems beeinträchtigen, insbesondere, wenn sie nicht gründlich getestet wurden.
- **Hohe Kosten:** Die Notwendigkeit, schnell zu handeln, kann zusätzliche Kosten verursachen, z.B. durch Überstunden oder den Einsatz externer Experten.

Zentrale Fragen sind u.a.:

- Was passiert, wenn wir die Änderung nicht durchführen?
- Was passiert, wenn die Änderung durchgeführt wird?

Es ist wichtig, diese Nachteile abzuwägen und sicherzustellen, dass E-Changes nur dann durchgeführt werden, wenn sie wirklich notwendig sind

Freigabe

Die Freigabe wird entweder schriftlich (E-Mail oder ITSM Tool) oder durch ein E-CAB erteilt. Bei den *Auftraggebern* hat die Rolle Emergency Change Manager die Befugnis, eine Freigabe zu erteilen.

Die Rolle haben folgende Funktionsrollen:

- Change Manager

- IT Major Incident Manager
- Senior Manager
- Manager von Dienst MvD (24/7-365)
- Bereichsleitung

Zusammenstellung des ECAB

Das ECAB besteht aus Mitgliedern, die aufgrund ihrer Expertise und Verfügbarkeit ausgewählt werden. Dies können Vertreter aus verschiedenen IT-Bereichen, dem Business und externen Partnern sein. Die Teilnehmer beraten den E-Change Manager, um hinsichtlich der Geschäftsfähigkeit eine Entscheidung treffen zu können.

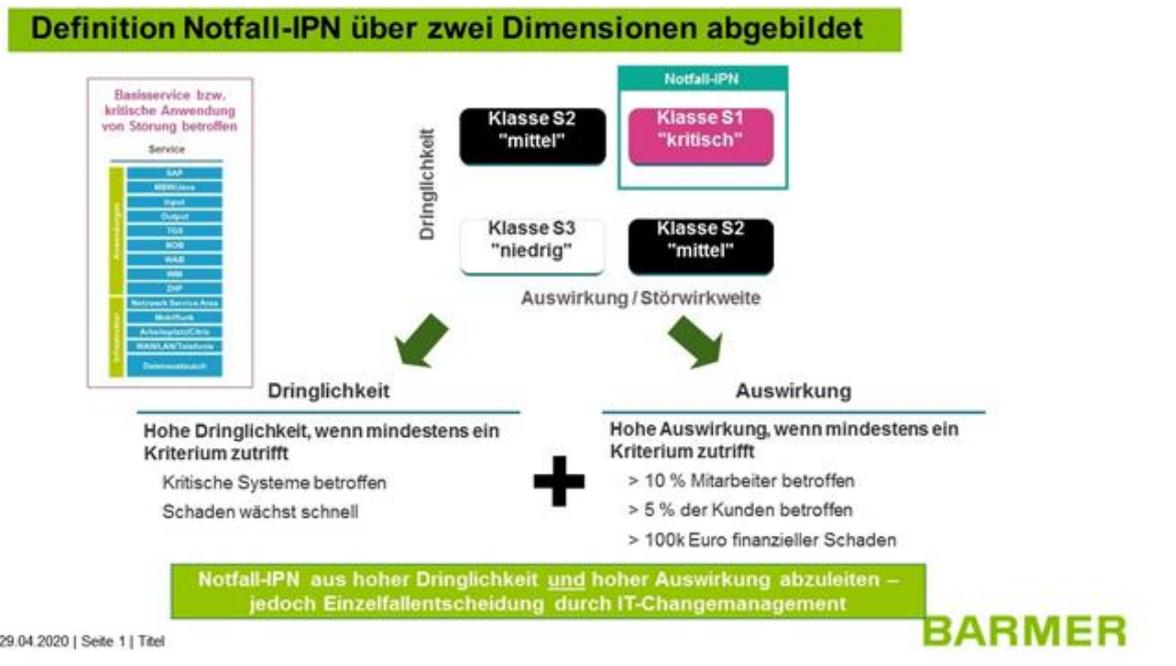
Dokumentation

Die Dokumentation wird im ITSM Tool durchgeführt. Bedingt durch die Eilbedürftigkeit darf ein E-Change auch im Nachgang dokumentiert werden. Spätestens muss eine vollständige Dokumentation nach 2 Werktagen nach Behebung des Vorfalls vorliegen.

Dienstleister

Dienstleister können unter bestimmten Bedingungen selbstständig E-Changes durchzuführen. Das hängt jedoch von den vertraglichen Vereinbarung ab.

E-Change in Jira (gilt nur für die BARMER)



Bei der Bewertung einer Notfall-IPN sind zur **Auswirkung / Störwirkweite** die folgenden drei Punkte zu berücksichtigen:

- Anzahl beeinträchtigter Mitarbeiter
- Anzahl betroffener Kunden / Geschäftspartner bzw. Beeinträchtigung der Außenwirkung
- Voraussichtlicher finanzieller Schaden

Des Weiteren ist die Dringlichkeit der Störungsbehebung zu bewerten. Bei der Bewertung der Dringlichkeit sind die folgenden drei Punkte zu berücksichtigen:

- Zeitliche Entwicklung des Schadens
- Betroffener Geschäftsprozess
- Existenz von Umgehungslösungen (Workarounds)

	Störfweite	Dringlichkeit
Hoch	<ul style="list-style-type: none"> • Eine große Anzahl von Mitarbeitern ist von der IT-Störung betroffen (>10%), die dadurch nicht mehr arbeiten kann. • Eine große Anzahl von Kunden (> 5%) ist von der IT-Störung betroffen und dadurch in irgendeiner Art und Weise beeinträchtigt. • Der voraussichtlich entstehende finanzielle Schaden durch die IT-Störung ist hoch (> 100.000 EUR) • 30% der Funktionalitäten eines Kernsystems sind betroffen. • Der Reputationsschaden für die BARMER ist hoch. 	<ul style="list-style-type: none"> • Der durch die IT-Störung entstehende Schaden wächst zeitlich sehr schnell. • Die Arbeit, die durch die IT-Störung nicht erledigt werden kann, ist zeitkritisch. • Mehrere Anwender mit VIP-Status (definierte Funktionsträger) sind betroffen.
Niedrig	<ul style="list-style-type: none"> • Eine kleine Anzahl von Mitarbeitern ist von der IT-Störung betroffen (<= 10%), denen dadurch in ihrer Arbeit Extra- Aufwände entstehen. • Eine kleine Anzahl von Kunden ist von der IT-Störung betroffen (<= 5%), die dadurch in unwesentlicher Art und Weise Unannehmlichkeiten haben. • Der voraussichtlich entstehende finanzielle Schaden durch die IT-Störung ist gering (<= 100.000 EUR). • Der Reputationsschaden für die BARMER ist gering. 	<ul style="list-style-type: none"> • Der durch die IT-Störung entstehende Schaden wächst nicht oder zeitlich nur sehr langsam. • Die Arbeit, die durch die IT-Störung nicht erledigt werden kann, ist nicht zeitkritisch. • Eine Umgehungslösung (Work-around) existiert und den Betroffenen bekannt.

Die vorstehend dargestellte Bewertungsmethodik und die Klassifizierung der zwei Kriterien sind Indikativ zu verstehen und im Einzelfall situationsabhängig auszulegen. Die Entscheidung, ob eine Notfall-IPN vorliegt, liegt in der Verantwortung des IT-Changemanagement und kann z.B. auch auf Basis der Erfahrung oder durch die Störungshistorie beeinflusst werden.

Eine Notfall-IPN muss innerhalb von 3 Tagen nach dem Antrag fertig gestellt (Status Fachtest abgeschlossen) werden. Die NIPNs die nicht rechtzeitig fertig gestellt werden, werden abgelehnt. Diese können dann gerne über die fast wöchentlichen F&Fs eingespielt werden.

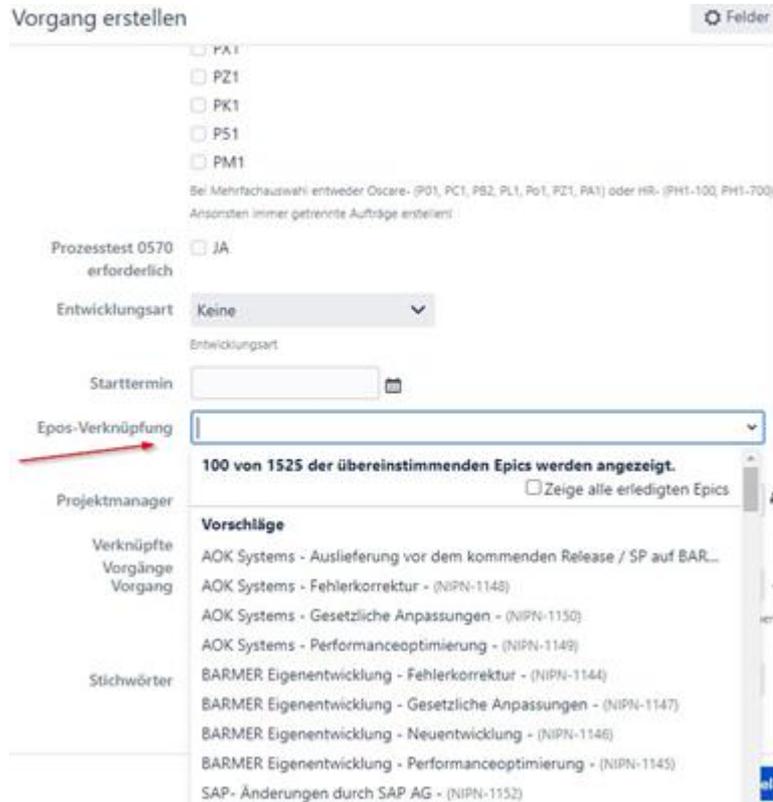
Zur Erfassung einer NOTFALL-IPN in JIRA sind folgende Informationen im Beschreibungsfeld zu erfassen:

- Welche Beeinträchtigung liegt vor? Beschreiben sie das Fehlerbild
- Welcher **Technical Service Offering (TSO)** ist betroffen?
- Wie hoch ist die Auswirkung?
 - Anzahl der beeinträchtigten Benutzer?
 - Welcher Geschäftsprozess ist betroffen?
- Seit wann besteht das Problem?
- Welche Ticket-Nummer oder RQM Nummer existiert zu dieser Beeinträchtigung?
- Gibt es bereits ein alternatives Vorgehen (Workaround) und wie sieht es aus?
- Was muss zur Lösung der Beeinträchtigung getan werden?
- Warum kann der Transport nicht bis zum nächsten F&F warten?
- Wann soll die Notfall-IPN durchgeführt werden?
- Gibt es bei der Umsetzung eine Einschränkung der Services (Dauer)?
- Gibt es Abhängigkeiten, die berücksichtigt werden müssen?
 - Dialog?
 - PKM TV?
 - Claims TV?
 - sonstiges?
 - Löschung von System-Cache ja/nein
 - Neuanlage von Datenbank/Tabellen-Indizes ja/nein
 - Risiko Betrachtung
 - Gibt für die Umsetzung erkannte Risiken?
 - Wurden Gegenmaßnahmen getroffen?
 - Welche Fallback Strategie gibt es?
- Kontakt im Notfall (technisch, fachlich)
- Wurde die EPOS Version eingetragen?

Für die Qualitätssicherung und Reduzierung der NIPNs ist es notwendig ab sofort die EPOS Version mit auszufüllen

Damit möchten wir feststellen, woher die Notfall IPNs ihren Ursprung haben.

Beispiel:



EChange in ServiceNow (gilt nur für die HEK)

Analog zur v.g. BARMER ist die Definition der Notfall-Pin aus den Dimensionen hohe Dringlichkeit und hohe Auswirkungen abzuleiten.

Bei der Bewertung einer Notfall-IPN sind zur **Auswirkung / Störwirkweite** die folgenden drei Punkte zu berücksichtigen:

- Anzahl beeinträchtigter Mitarbeiter
- Anzahl betroffener Kunden / Geschäftspartner bzw. Beeinträchtigung der Außenwirkung
- Voraussichtlicher finanzieller Schaden

Des Weiteren ist die Dringlichkeit der Störungsbehebung zu bewerten. Bei der Bewertung der Dringlichkeit sind die folgenden drei Punkte zu berücksichtigen:

- Zeitliche Entwicklung des Schadens
- Betroffener Geschäftsprozess
- Existenz von Umgehungslösungen (Workarounds)

	Störwirkweite	Dringlichkeit
Hoch	<ul style="list-style-type: none"> • Eine große Anzahl von Mitarbeitern ist von der IT-Störung betroffen (>10%), die dadurch nicht mehr arbeiten kann. • Eine große Anzahl von Kunden (> 5%) ist von der IT-Störung betroffen und dadurch in irgendeiner Art und Weise beeinträchtigt. • Der voraussichtlich entstehende finanzielle Schaden durch die IT-Störung ist hoch (> 100.000 EUR) • 30% der Funktionalitäten eines Kernsystems sind betroffen. • Der Reputationsschaden für die HEK ist hoch. 	<ul style="list-style-type: none"> • Der durch die IT-Störung entstehende Schaden wächst zeitlich sehr schnell. • Die Arbeit, die durch die IT-Störung nicht erledigt werden kann, ist zeitkritisch. • Mehrere Anwender mit VIP-Status (definierte Funktionsträger) sind betroffen.
Niedrig	<ul style="list-style-type: none"> • Eine kleine Anzahl von Mitarbeitern ist von der IT-Störung betroffen (<= 10%), denen dadurch in ihrer Arbeit Extra- Aufwände entstehen. • Eine kleine Anzahl von Kunden ist von der IT-Störung betroffen (<= 5%), die dadurch in unwesentlicher Art und Weise Unannehmlichkeiten haben. • Der voraussichtlich entstehende finanzielle Schaden durch die IT-Störung ist gering (<= 100.000 EUR). • Der Reputationsschaden für die HEK ist gering. 	<ul style="list-style-type: none"> • Der durch die IT-Störung entstehende Schaden wächst nicht oder zeitlich nur sehr langsam. • Die Arbeit, die durch die IT-Störung nicht erledigt werden kann, ist nicht zeitkritisch. • Eine Umgehungslösung (Work-around) existiert und den Betroffenen bekannt.

Die vorstehend dargestellte Bewertungsmethodik und die Klassifizierung der zwei Kriterien sind Indikativ zu verstehen und im Einzelfall situationsabhängig auszulegen. Die Entscheidung, ob eine Notfall-IPN vorliegt, liegt in der Verantwortung des IT-Changemanagement und kann z.B. auch auf Basis der Erfahrung oder durch die Störungshistorie beeinflusst werden.

Eine Notfall-IPN muss innerhalb von 3 Tagen nach dem Antrag fertig gestellt (Status Fachtest abgeschlossen) werden. Die NIPNs die nicht rechtzeitig fertig gestellt werden, werden abgelehnt.

Zur Erfassung einer NOTFALL-IPN sind folgende Informationen im Beschreibungsfeld zu erfassen:

- Welche Beeinträchtigung liegt vor? Beschreiben sie das Fehlerbild
- Welcher **Technical Service Offering (TSO)** ist betroffen?
- Wie hoch ist die Auswirkung?

- o Anzahl der beeinträchtigten Benutzer?
 - o Welcher Geschäftsprozess ist betroffen?
- Seit wann besteht das Problem?
- Welche Ticket-Nummer Nummer existiert zu dieser Beeinträchtigung?
- Gibt es bereits ein alternatives Vorgehen (Workaround) und wie sieht es aus?
- Was muss zur Lösung der Beeinträchtigung getan werden?
- Wann soll die Notfall-IPN durchgeführt werden?
- Gibt es bei der Umsetzung eine Einschränkung der Services (Dauer)?
- Gibt es Abhängigkeiten, die berücksichtigt werden müssen?
 - o Dialog?
 - o PKM TV?
 - o Claims TV?
 - o sonstiges?
 - Löschung von System-Cache ja/nein
 - Neuanlage von Datenbank/Tabellen-Indizes ja/nein
 - o Risiko Betrachtung
 - o Gibt für die Umsetzung erkannte Risiken?
 - o Wurden Gegenmaßnahmen getroffen?
 - o Welche Fallback Strategie gibt es?
- Kontakt im Notfall (technisch, fachlich)