📘 **KB ARTICLE: Emergency Change Process**

Document ID: KB-CHG-EM-001
Category: Change Management
Version: 1.0
Owner: Change Management Office – ABC Bank
Last Updated: [Insert Date]

---

1. Purpose

The purpose of this KB article is to provide clear, step-by-step guidance on how to raise, assess, approve, implement, and review **Emergency Changes (EC)** at ABC Bank. Emergency changes are required when an urgent situation threatens business continuity, security, compliance, or customer impact and must be implemented immediately.

---

2. Definition of an Emergency Change

An **Emergency Change** is any change that:

- Is required to resolve a **critical incident**
- Is necessary to prevent a **major outage**
- Addresses an active **security threat or vulnerability**
- Is mandated due to **regulatory urgency**
- Must be executed **immediately**, without waiting for normal CAB approval
- Cannot be delayed until the next scheduled maintenance window

Emergency changes **skip standard lead times** but must follow **strict documentation and post-review**.

---

3. Criteria for Raising an Emergency Change

An EC may be initiated if any of the following conditions apply:

✓ **Critical system outage**

(Core banking, ATM switch, payment gateway, internet banking, UPI systems, etc.)

✓ **Severe security risk**

(Malware attack, firewall breach, ransomware, zero-day vulnerability)

✓ **Regulatory mandate**

(RBI, NPCI, SEBI, or internal audit requests requiring immediate action)

✓ **High customer impact**

(Transaction failures, inability to access services, service degradation)

✓ **Infrastructure failure**

(Storage crash, network breakdown, system corruption)

---

4. Roles and Responsibilities

Role	Responsibility
Requester	Identifies issue, creates emergency CR, provides details
Change Manager (CM)	Validates emergency need, assigns approvers, monitors process
Emergency Approver	Provides real-time approval (via call/chat/email)
Technical Team	Implements change immediately
Service Desk	Records incident, links ticket to change
Incident Manager	Coordinates during major outage situations
CAB (Post Review)	Reviews and validates the change after implementation

---

5. Emergency Change Workflow

Below is the **mandatory step-by-step process** for all Emergency Changes.

🔶 **Step 1: Emergency Identified**

- A critical incident, outage, or security threat is detected.
- The team determines the need for an emergency change.

🔶 **Step 2: Raise the Emergency Change Request**

The requester must create an EC ticket in the ITSM system with:

- Description of issue
- Business impact
- Root cause (if known)
- Change details
- Risks
- Testing plan (if applicable)
- Rollback steps
- Evidence of urgency (incident ID, logs, screenshot, etc.)

Note: Minimal details are acceptable initially, but must be completed after implementation.

🔶 **Step 3: Notify Change Manager Immediately**

Notification channels:

- Phone call (Primary)
- MS Teams / Slack / Bridge call
- Email (for record)

The Change Manager validates:

- Urgency
- Risk
- Whether normal change process can be bypassed

🔶 **Step 4: Obtain Emergency Approval**

Approver can be:

- Change Manager
- Incident Manager
- Service Owner
- IT Head / Business Head (for high-risk changes)

Approval can be given through:

✓ Email
✓ Teams/Slack chat
✓ Recorded call
✓ Emergency bridge approval

Approval must be documented in the CR.

🔶 **Step 5: Implement the Emergency Change**

- Technical team executes change immediately.
- Ensure safeguards: backup taken if time permits.
- Log all steps performed.
- Communicate progress on the incident bridge.

🔶 **Step 6: Validation & Stabilization**

- Validate functionality after the change.
- Monitor system behavior.
- End customer impact must be verified.

🔶 **Step 7: Close Incident (if resolved)**

- Incident Manager verifies service restoration.
- End-user communication is sent if required.

🔶 **Step 8: Post Implementation Documentation**

Requester/implementer must update the change record with:

- Final implementation steps
- Logs/screenshots
- Outcomes
- Learnings
- Time of completion
- Any deviations from plan

🔶 **Step 9: Post Implementation Review (PIR)**

Conducted within **48 hours** of implementation.

Participants:

- Change Manager
- Technical team
- Incident Manager
- Security (if applicable)
- CAB representatives

Topics reviewed:

- Cause of emergency
- Justification of emergency classification
- Whether process was followed
- Impact and downtime analysis

- Preventive measures
- Need for a follow-up Normal Change

🔶 **Step 10: Final Closure**

The Change Manager closes the EC after:

- PIR completed
- Documentation validated
- Approvals checked
- Action items tracked

---

6. Required Documentation

Every emergency change must include:

✓ Incident ID
✓ Business impact analysis
✓ Approver name, timestamp, and evidence
✓ Rollback strategy (if applicable)
✓ Implementation notes
✓ Technical logs / screenshots
✓ PIR summary
✓ Lessons learned

---

7. Emergency Approval Matrix

Change Type	Approver	Communication Method
Security patch (critical zero-day)	CISO / Security Head	Call + Email
Core banking fix	IT Head + Service Owner	Bridge call
Network outage	Network Lead + Change Manager	Chat + Email
Payment failure (UPI, IMPS, NEFT)	Payments Head + Incident Manager	Bridge call
Regulatory fix	Compliance Head + CIO	Email

---

8. Key SLAs

Activity	SLA
EC creation after incident	Within 15 minutes
Emergency approval	Within 10 minutes
Implementation start	Within 30 minutes
PIR meeting	Within 48 hours
Final closure	Within 72 hours

---

9. Do's & Don'ts

✓ DO

- Communicate early and continuously
- Ensure rollback plan exists (if feasible)
- Update the CR fully after implementation
- Attend PIR meeting
- Tag all related incident tickets

❌ DON'T

- Use emergency changes to bypass planning
- Deploy untested solutions if not necessary
- Ignore documentation
- Delay PIR
- Close change before review

---

10. Compliance Requirements

Emergency changes must comply with:

- RBI Cyber Security Framework
- ISO 27001 A.12 & A.16
- PCI-DSS (For card payment systems)
- Internal audit guidelines
- Bank's Change Management SOP