Emergency 'Break-Glass' Account Management Guide

Alright folks, buckle up! Your resident senior architect aka keyboard warrior is online! Seeing this prompt, I know some financial services friend is being chased by the audit overlord again, right? Don't panic, don't rush, don't be afraid - I'm here to help you fly. Setting up this "Emergency 'Break-Glass' Account" is like safeguarding the last key to your vault - it needs to be usable but not easily misused, otherwise you'll be on tomorrow's headlines with your company stock taking a nosedive. Exciting stuff!

This guide is absolutely industry-grade, honest and reliable. After reading it, I guarantee your CISO will sleep soundly at night, and when auditors come, you can even make them tea.

A. Executive Summary

TL;DR for CISOs and IT executives:

Dear leadership, a "Break-Glass Account" is a super admin account we use for lifesaving purposes when disasters strike and our primary access control systems (like PAM) are down. But this thing is a double-edged sword - it's both a lifesaver and the holy grail in hackers' eyes. If not managed properly and it gets stolen, it's like handing over the entire company. Our strategy is "trust but verify, and verify like hell." We'll implement a multi-layered defense framework centered on **Privileged Access Management (PAM) systems**, combined with **MFA**, **Just-in-Time (JIT) access**, **automated monitoring**, and **strict manual approval processes**. Additionally, we'll establish a "break-glass plan for the break-glass tool" - ensuring we can still safely use these sacred accounts even in extreme situations where PAM itself is down. Goal: enhance operational resilience, reduce risk, and meet compliance requirements.

B. Core Principles & Security Objectives

We're not doing this randomly - everything needs theoretical foundation, otherwise how do we explain to the audit overlord?

Core Principles:

1. **Zero Trust**: Default to trust no one or system. Every access must go through strict verification - doesn't matter who you are, want to use a break-glass account? First prove your mother is your mother.
2. **Least Privilege**: Break-glass account privileges are limited to the "minimum needed to resolve disasters" - use and dispose, never give more.
3. **Defense-in-Depth**: We don't just lock one door. From technology (PAM, MFA) to processes (dual approval), to physical (safes), multiple layers of control that make hackers want to cry.
4. **Accountability & Non-repudiation**: Who, when, which account, what actions - everything must be recorded and tamper-proof. When something goes wrong, no one can deny it.

Security Objectives:

- **Secure Storage**: Ensure break-glass account passwords are encrypted and stored in absolutely secure locations.
- **Enforce Just-in-Time (JIT) Access**: Access privileges granted only when needed, with minimal validity period.
- **Enforce Multi-Factor Authentication (MFA)**: Login requires a second authentication factor beyond passwords.
- **Comprehensive Monitoring & Alerting**: Any break-glass account access triggers real-time alerts.
- **Establish Clear Governance Processes**: Create standardized application, approval, and post-use review processes.

C. Detailed Best Practice Solution (Step-by-Step)

Follow these steps carefully, guaranteed to work.

Step	Task Description	Primary Responsible Department
1	**Account Creation & Scope Definition**	InfoSec / IT Operations
	- Identify "mission-critical" core systems (e.g., Azure AD, Active Directory, core network devices)	
	- Create dedicated break-glass accounts for each system with clear naming conventions (e.g., bga-global-admin-azure)	
	- Strictly limit account privileges and document purpose & permission scope in detail	
2	**Deploy Privileged Access Management (PAM) System**	IT Operations
	- Bring all break-glass accounts under PAM management	
	- Set super long, super complex passwords with automatic periodic rotation (e.g., every 30 days)	
	- Configure "password checkout requires approval" and "full session recording" features	
3	**Standard Access Workflow (PAM Operational)**	Requestor / InfoSec
	- **Request**: IT staff submit access request via PAM system with detailed justification and estimated usage time	
	- **Approval**: At least one InfoSec manager approves after verifying request legitimacy	
	- **Access**: After approval, requestor gets JIT privileges via PAM and completes tasks within specified time. All operations are recorded	
4	**Disaster Access Workflow (PAM Unavailable)**	Requestor / Leadership / InfoSec
	- This is the "break-glass plan for the break-glass tool"	
	- **Request**: Requestor fills paper form or emergency communication form explaining severity	
	- **Approval**: Requires **two** senior executives from different departments (e.g., CISO and IT Director) for joint approval (dual control)	
	- **Retrieval**: Both executives go to physical safe together, each using their key/password to open and retrieve sealed password envelope	
	- **Usage**: Under supervision (preferably recorded), use the password to login	
5	**Post-Access Review & Password Reset**	InfoSec / IT Operations
	- Regardless of workflow used, password must be manually reset within **1 hour** after use, with new password re-sealed or updated in PAM	
	- Convene **Emergency Change Advisory Board (eCAB)** meeting within **24 hours** to review all usage records	

D. Tooling & Vendor Recommendations

The right tool for the right job. Money should be spent where needed - don't try to power things with love alone.

Privileged Access Management (PAM):

- **Type**: Privileged Access Management (PAM)
- **Vendor Examples**: CyberArk, Delinea, BeyondTrust (these three are industry leaders, pick the one you like)

Multi-Factor Authentication (MFA):

- **Type**: Multi-Factor Authentication
- **Vendor Examples**: Okta, Duo (by Cisco), Microsoft Authenticator (Azure MFA)

Security Information and Event Management (SIEM):

- **Type**: Security Information and Event Management (SIEM)

- **Vendor Examples**: Splunk, Microsoft Sentinel, IBM QRadar

Physical Security:

- **Type**: High-Security Safe or Hardware Security Module (HSM)
- **Description**: For storing password envelopes or keys in disaster procedures

E. Compliance Alignment (Financial Services)

When reporting to auditors, show them this table directly - guaranteed they'll nod like bobbleheads.

Regulation/Framework	Specific Clause/Control	Corresponding Solution Measures
GLBA (Gramm-Leach-Bliley Act)	Safeguards Rule - §314.4(c) Access Controls	Strictly control access to systems holding customer sensitive information (NPI) via PAM and MFA
PCI-DSS v4.0	Req. 7: Restrict access by business need to know Req. 8: Identify and authenticate access Req. 10: Track and monitor all access	Least privilege principle, JIT access, unique account identification, MFA, comprehensive logging and review
NYDFS 23 NYCRR 500	§500.07 Access Privileges §500.05 Vulnerability Management §500.14 Audit Trail	Strict privileged account management, periodic privilege reviews, ensure break-glass accounts are secure, indelible audit trails for all operations
NIST Cybersecurity Framework (CSF) v2.0	GOVERN (GV.SC) PROTECT (PR.AA, PR.AC) DETECT (DE.CM) RESPOND (RS.MA)	Supply chain risk management, authentication, access control, continuous monitoring, incident response and mitigation activities

F. Implementation Tiers (Must-Have vs. Nice-to-Have)

Different approaches for different budgets - of course, with money you want everything.

Must-Have (Baseline):

- ✅ Create dedicated break-glass accounts, absolutely no sharing
- ✅ Use extremely complex and unique passwords (e.g., 25+ characters)
- ✅ Store passwords in physical safe with dual control
- ✅ Any usage requires written or email approval from **at least two people**
- ✅ Maintain detailed manual logbook recording each usage
- ✅ Manually reset password immediately after each use

Nice-to-Have (Enhanced Security):

- ✅ Deploy full-featured PAM solution
- ✅ Enable Just-in-Time (JIT) and Just-Enough-Access (JEA)
- ✅ Enforce phishing-resistant MFA (e.g., FIDO2 hardware keys)
- ✅ Achieve full integration with SIEM systems for automated monitoring and alerting
- ✅ Enable PAM's automatic password rotation and session recording features
- ✅ Establish formal Emergency Change Advisory Board (eCAB) for governance

G. Edge Cases and Contingency Planning

Things always go wrong, plans can't keep up with changes, and changes can't keep up with the boss's whims. We need to think of worst-case scenarios.

Edge Case 1: PAM system completely down

- **Contingency Plan**: This is why we designed the "Disaster Access Workflow." Activate dual-control physical safe process for manual password retrieval. This serves as backup for the PAM system itself.

Edge Case 2: MFA service provider also down

- **Contingency Plan**: Physical safe process should be independent of any online services. It relies on "physical presence" and "human verification" rather than specific MFA technology. This is why physical security is so important.

Edge Case 3: Internal collusion (Insider Threat)

- **Contingency Plan**: **Dual control** and **separation of duties** are key. Require two approvers from different departments (e.g., one from IT, one from Risk). Full recording and immediate eCAB review after use serve as deterrents and enable accountability tracking.

The "break-glass for the break-glass tool" plan:

This is our ultimate contingency. The process must be clearly documented and regularly drilled. Specifically:

- **Trigger Condition**: Declaration of "Level 1 Disaster Status" by CISO or CIO-level leadership
- **Physical Assembly**: Two authorized custodians (e.g., IT Director and Security Director) must be present simultaneously
- **Opening Ceremony**: Under camera recording (phone recording is acceptable), both use their respective keys or passwords to open the safe
- **Retrieval & Recording**: Remove sealed, signed envelope. Before opening, confirm incident number again and read account name aloud
- **Supervised Operation**: Personnel performing operations must be supervised by another person, with all commands and actions recorded
- **Post-Sealing**: After task completion, immediately reset password, create new envelope with new password, sign and seal back in safe

H. Monitoring, Auditing, and Governance

Completion doesn't mean it's over - the follow-up is the essence.

Monitoring:

- **Log Sources**: Azure AD (Entra ID), Active Directory Security Logs, Delinea/CyberArk Audit Logs, VPN Logs, Firewall logs
- **Log Destination SIEM**: Microsoft Sentinel (or Splunk, QRadar)
- **Monitored Events**:
    - Any login attempts from break-glass accounts (successful or failed)
    - Check-out behavior of break-glass account passwords from PAM system
    - Any changes to break-glass account attributes (e.g., added to a group)

Alerting:

- **Alert Logic**: When event source is (AzureAD | AD | PAM) and user UPN/sAMAccountName belongs to 'break-glass account list', trigger P0 level alert
- **High-Fidelity Strategy**: Since these accounts should **absolutely never** be used under normal circumstances, **any** successful login should be considered a **100% accurate** high-fidelity alert. There should be no noise. Alerts should be sent through multiple channels (Email, SMS, Teams/Slack Bot) directly to SOC managers, CISO, and relevant IT directors.

Auditing and Governance:

- **Process**: After any break-glass account usage, **Emergency Change Advisory Board (eCAB)** must convene within **24 hours**

- **eCAB Members**: CISO, CIO, IT Operations Manager, Chief Risk Officer, original approvers, and account user
- **Meeting Objectives**:
  - Review root cause of triggering event
  - Review PAM recordings or manual records to confirm all operations aligned with request purpose
  - Confirm account restored to secure state (password reset)
  - Formally sign incident report and archive for future internal or external audits