MFA Deployment Checklist

Password Security: From Weak Links to Strong Defense

A step-by-step implementation guide from First Underwriters Insurance Brokers

WHY MFA IS NON-NEGOTIABLE

Multi-factor authentication (MFA) is the single most effective control against credential-based attacks. Microsoft reports that MFA blocks **99.9% of automated attacks** on accounts. Cyber insurance carriers now treat MFA as a baseline requirement—organizations without comprehensive MFA deployment face coverage denials, exclusions, or significantly higher premiums.

This checklist guides you through planning, deploying, and validating MFA across your organization's critical systems.

Organization: _____

Project Lead: _____

Target Completion Date: _____

Date Started: _____

Phase 1: Pre-Deployment Planning

1.1 Inventory and Assessment	
[ ]	Complete inventory of all user accounts (employees, contractors, vendors)
[ ]	Identify all systems requiring MFA (email, VPN, cloud apps, admin consoles)
[ ]	Document current authentication methods for each system
[ ]	Classify accounts by risk level (standard user, privileged, service)
[ ]	Identify legacy systems that may not support modern MFA
[ ]	Calculate total number of MFA licenses/tokens required
[ ]	Document existing password policies and identify gaps

1.2 MFA Solution Selection	
[ ]	Evaluate MFA solutions against organizational requirements
[ ]	Verify compatibility with all target systems (IdP, VPN, SaaS, on-prem)
[ ]	Confirm support for preferred authentication methods (FIDO2, TOTP, push)
[ ]	Review vendor security certifications (SOC 2, ISO 27001)
[ ]	Obtain pricing and licensing structure (per-user, per-device, enterprise)
[ ]	Evaluate self-service enrollment and recovery capabilities
[ ]	Confirm integration with existing identity provider (Azure AD, Okta, etc.)
[ ]	Document vendor support SLAs and escalation procedures

This checklist is provided as a risk management resource. It does not constitute technical or legal advice.

1.3 Stakeholder Alignment	
[ ]	Obtain executive sponsorship and budget approval
[ ]	Brief IT leadership on timeline and resource requirements
[ ]	Coordinate with HR on employee communication plan
[ ]	Engage legal/compliance on policy updates and documentation
[ ]	Identify department champions to assist with rollout
[ ]	Establish project governance and escalation path

Phase 2: Technical Preparation

2.1 Infrastructure Readiness	
[ ]	Configure identity provider for MFA enforcement
[ ]	Set up MFA administration console and admin accounts
[ ]	Configure conditional access policies (location, device, risk)
[ ]	Establish backup authentication methods (recovery codes, backup phone)
[ ]	Test integration with each target system in staging environment
[ ]	Configure logging and monitoring for MFA events
[ ]	Set up alerting for suspicious authentication patterns
[ ]	Document rollback procedures if issues arise

2.2 Privileged Account Preparation	
[ ]	Procure hardware security keys for all privileged accounts
[ ]	Register backup hardware keys for each privileged user
[ ]	Configure break-glass emergency access procedures
[ ]	Test emergency access credentials in isolated environment
[ ]	Document privileged account MFA procedures
[ ]	Train IT staff on privileged MFA recovery scenarios

2.3 User Communication Preparation	
[ ]	Create enrollment instructions with screenshots
[ ]	Prepare FAQ document for common questions
[ ]	Develop troubleshooting guide for helpdesk
[ ]	Create email templates for rollout announcements
[ ]	Schedule training sessions (live and recorded options)
[ ]	Set up dedicated support channel (email, chat, phone)
[ ]	Prepare executive talking points for all-hands communication

2.4 Approved MFA Methods Reference

This checklist is provided as a risk management resource. It does not constitute technical or legal advice.

Security Tier	Method	Examples	Notes
Tier 1 (Highest)	FIDO2 Hardware Key	YubiKey, Titan, Feitian	Phishing-resistant; required for privileged accounts
Tier 2	Authenticator App (TOTP)	Microsoft Auth, Google Auth	Strong protection; recommended for standard users
Tier 3	Push Notification	Duo, Okta Verify	Must use number-matching; simple approve/deny not acceptable
Not Approved	SMS / Voice OTP	Text message codes	Vulnerable to SIM swap; do not use
Not Approved	Email OTP	Codes sent to email	Circular dependency; do not use

Phase 3: Rollout Execution

Deploy MFA in waves to manage support load and identify issues early.

3.1 Wave 1: IT and Security Team (Pilot)	
[ ]	Enroll IT and security team members first
[ ]	Test all target systems with MFA enabled
[ ]	Document any integration issues or edge cases
[ ]	Refine enrollment instructions based on feedback
[ ]	Update FAQ and troubleshooting guide
[ ]	Verify helpdesk is prepared for user support
[ ]	Confirm monitoring and alerting is functional

3.2 Wave 2: Executive Leadership	
[ ]	Provide white-glove enrollment support for executives
[ ]	Issue hardware security keys to all executives
[ ]	Ensure executive assistants have backup access procedures
[ ]	Brief executives on security rationale and insurance requirements
[ ]	Document any executive-specific workflow considerations

3.3 Wave 3: High-Risk Roles	
[ ]	Enroll finance/accounting team (BEC target mitigation)
[ ]	Enroll HR team (W-2/payroll fraud prevention)
[ ]	Enroll IT administrators (privileged access protection)
[ ]	Enroll anyone with access to sensitive data or financial systems
[ ]	Verify MFA is enforced on all financial applications

3.4 Wave 4: General Population	
[ ]	Send enrollment notification to remaining employees
[ ]	Set enrollment deadline (recommended: 14 days)
[ ]	Monitor enrollment progress daily

This checklist is provided as a risk management resource. It does not constitute technical or legal advice.

[ ]	Send reminder emails at 7 days, 3 days, 1 day before deadline
[ ]	Provide drop-in support sessions for stragglers
[ ]	Escalate non-compliant users to management
[ ]	Enable MFA enforcement after deadline

3.5 Contractors and Vendors	
[ ]	Notify contractors of MFA requirement
[ ]	Provide enrollment instructions for external users
[ ]	Verify contractor IdP supports MFA (if federated)
[ ]	Set enforcement date for contractor access
[ ]	Update vendor contracts to require MFA

Phase 4: Post-Deployment Validation

4.1 Coverage Verification	
[ ]	Run report showing all accounts with MFA enabled
[ ]	Identify any accounts without MFA (should be zero or documented exceptions)
[ ]	Verify MFA is enforced on all external-facing systems
[ ]	Confirm VPN requires MFA for all connections
[ ]	Verify cloud admin consoles require MFA
[ ]	Test MFA enforcement by attempting access without second factor
[ ]	Document any approved exceptions with risk acceptance

4.2 Security Testing	
[ ]	Attempt authentication bypass (ensure MFA cannot be skipped)
[ ]	Test session timeout and re-authentication requirements
[ ]	Verify MFA events are logged correctly
[ ]	Test alerting for failed MFA attempts
[ ]	Verify impossible travel detection is functional
[ ]	Test account lockout after failed MFA attempts
[ ]	Conduct phishing simulation targeting MFA credentials

4.3 Documentation and Evidence	
[ ]	Screenshot MFA configuration for all critical systems
[ ]	Export enrollment report showing 100% coverage (or documented exceptions)
[ ]	Document conditional access policies
[ ]	Save evidence of hardware key distribution for privileged accounts
[ ]	Update security policies to reflect MFA requirements
[ ]	Create executive summary for cyber insurance documentation

This checklist is provided as a risk management resource. It does not constitute technical or legal advice.

4.4 Deployment Metrics

Metric	Value	Notes
Total accounts in scope		
Accounts with MFA enabled		
MFA coverage percentage		Target: 100%
Approved exceptions (documented)		Target: < 1%
Hardware keys distributed (privileged)		
Helpdesk tickets during rollout		
Failed enrollments requiring support		
Days from start to full enforcement		

Phase 5: Ongoing Operations

5.1 Continuous Monitoring	
[ ]	Review MFA authentication logs weekly for anomalies
[ ]	Monitor for accounts with MFA disabled or bypassed
[ ]	Track MFA failures and investigate patterns
[ ]	Alert on impossible travel or suspicious locations
[ ]	Audit conditional access policy effectiveness monthly
[ ]	Review and close MFA exceptions at 90-day intervals

5.2 User Lifecycle Management	
[ ]	Include MFA enrollment in new hire onboarding (Day 1)
[ ]	Revoke MFA credentials on employee termination (same day)
[ ]	Re-enroll users on device replacement or loss
[ ]	Conduct quarterly access reviews including MFA status
[ ]	Update procedures for role changes affecting MFA requirements

5.3 Incident Response Integration	
[ ]	Add MFA compromise scenarios to incident response playbook
[ ]	Document procedure for emergency MFA bypass (break-glass)
[ ]	Train helpdesk on social engineering attempts to bypass MFA
[ ]	Establish verification procedures for MFA reset requests
[ ]	Test MFA-related incident response scenarios annually

This checklist is provided as a risk management resource. It does not constitute technical or legal advice.

CYBER INSURANCE DOCUMENTATION

Keep the following evidence for cyber insurance applications and renewals:

- **Coverage report** showing MFA enabled on 100% of accounts (or documented exceptions)
- **System list** with MFA enforcement status for all external-facing applications
- **Policy documentation** requiring MFA for remote access, email, and cloud services
- **Hardware key inventory** for privileged accounts
- **Exception register** with risk acceptance signatures and remediation timelines

Contact First Underwriters at **(425) 242-5357** for guidance on presenting your MFA deployment as part of a comprehensive cyber risk management program.

Common Issues and Troubleshooting

Issue	Resolution
User lost phone/authenticator	Use backup recovery codes; if unavailable, verify identity through manager and reset MFA enrollment
Hardware key not recognized	Verify USB connection; try different port; check if FIDO2 is enabled in browser/system; update firmware
Push notifications not arriving	Check device internet connection; verify app permissions; re-register device in MFA portal
MFA prompt not appearing	Clear browser cache; try incognito mode; verify conditional access policy applies; check for cached sessions
Legacy app cannot use MFA	Generate app-specific password if supported; otherwise document as exception with compensating controls
User traveling internationally	Pre-register travel in conditional access; ensure backup authentication method available; provide emergency contact
Account locked after MFA failures	Verify user identity; check for attack indicators; reset lockout; investigate if pattern across users
Contractor cannot enroll	Verify contractor IdP supports MFA; provide guest enrollment option; consider dedicated contractor tenant

This checklist is provided as a risk management resource. It does not constitute technical or legal advice.

Deployment Sign-Off

Confirm completion of all phases and obtain sign-off from responsible parties.

Phase / Milestone	Completed By	Date	Signature
Phase 1: Pre-Deployment Planning			
Phase 2: Technical Preparation			
Phase 3: Rollout Execution			
Phase 4: Post-Deployment Validation			
Phase 5: Ongoing Operations Established			
Final Approval			

First Underwriters Insurance Brokers
4055 Lake Washington Blvd NE, Suite 100, Kirkland, WA 98033
(425) 242-5357 | www.firstunderwriters.com

This checklist is provided as a risk management resource. It does not constitute technical or legal advice.