Change Management Policy

Table of contents

Title	Change Management Policy
Doc#	POL-CHANGE-001
Version	1.1
Date	05-05-2024
Supersedes	POL-CHANGE-001 v1.0 (12-02-2024)
Next Review	05-11-2024
Owner	Chief Technology Officer
Approved By	Chief Information Officer

ISO 27001 ALIGNMENT NOTE: This policy is intended to support ISO 27001:2022 compliance, specifically controls A.12.1.2 (Change management) and A.14.2.2 (System change control procedures). However, specific control mappings are incomplete.

RELATED POLICIES: This policy should be read in conjunction with: - Access Control Policy POL-SECU-021 (v1.3) - Incident Response Policy POL-SECU-010 (v2.1)
- Business Continuity Policy POL-BC-001 (v1.0) - Configuration Management Policy POL-CONFIG-001 (under development)

CloudCore change management policy establishes controlled processes for managing changes to information systems, infrastructure, and business processes to maintain security, stability, and

compliance. This policy applies to all changes affecting production systems, security controls, and business-critical processes.

> **SCOPE LIMITATION:** Policy states it applies to changes affecting production systems but later sections include development and testing environments without clear scope boundaries.

Policy Statement

CloudCore requires that:

(a) All changes to information systems and infrastructure follow formal change management procedures to ensure security and operational integrity.

(b) Changes are properly authorised, documented, tested, and reviewed before implementation.

(c) Emergency changes include appropriate controls and post-implementation review.

(d) Change management processes support business continuity and regulatory compliance requirements.

(e) Roles and responsibilities for change management are clearly defined and communicated.

> **ISO 27001 GAP:** Policy lacks explicit reference to ISO 27001 A.12.1.2 requirement for "formal change control procedures" including impact assessment and approval processes.

Change Categories

Standard Changes

Pre-approved changes with established procedures and minimal risk: - Routine software updates and patches - Pre-scheduled maintenance activities - Standard configuration changes - Approved hardware replacements

> **PRE-APPROVAL AUTHORITY:** Standard changes described as "pre-approved" but no authority specified for granting pre-approval status.

Normal Changes

Changes requiring formal assessment and approval: - New software installations - System configuration modifications - Process changes affecting multiple departments - Infrastructure upgrades and modifications

Emergency Changes

Urgent changes required to resolve critical issues: - Security incident remediation - Critical system failures - Urgent regulatory compliance requirements - Business continuity activations

> **EMERGENCY CRITERIA GAP:** Emergency change criteria not clearly defined, potentially allowing inappropriate use of expedited procedures.

Change Management Process

Change Request Initiation

1. Change requestor submits formal change request using approved template
2. Change request includes business justification and risk assessment
3. Initial impact analysis conducted by technical teams
4. Change categorised and assigned to appropriate approval workflow

> **TEMPLATE AVAILABILITY:** References "approved template" but no template provided or location specified in policy documentation.

Impact Assessment

All changes must include assessment of: - Security implications and control impacts - Business process dependencies and risks - Resource requirements (personnel, systems, budget) - Implementation timeline and rollback procedures - Compliance and regulatory considerations

> **ISO 27001 COMPLIANCE GAP:** Impact assessment doesn't explicitly address ISO 27001 A.14.2.2 requirement for "ensuring controls are not compromised" during system changes.

Change Approval Process

Standard Changes

- Approved through automated workflow
- Technical lead approval required
- Implementation scheduled through standard processes

Normal Changes

- Change Advisory Board (CAB) review and approval
- Security team assessment for security-relevant changes
- Business owner approval for process changes
- Final authorisation by Change Manager

CAB MEMBERSHIP GAP: Change Advisory Board referenced but membership, meeting frequency, and decision-making procedures not defined.

Emergency Changes

- Emergency Change Authority may approve immediately
- Security team consultation required for security-related changes
- Post-implementation review mandatory within 48 hours
- Formal change request submitted retrospectively

EMERGENCY AUTHORITY: Emergency Change Authority role mentioned but not defined elsewhere in policy or organisational structure.

Implementation Requirements

- Changes implemented according to approved schedule
- Implementation performed by authorised personnel only
- Progress monitored and documented throughout process
- Rollback procedures available and tested before implementation
- Post-implementation validation and testing completed

AUTHORISED PERSONNEL: References "authorised personnel" but no process defined for granting implementation authorisation.

Post-Implementation Review

- Verification that change objectives were achieved
- Assessment of any unexpected impacts or issues
- Documentation of lessons learned and process improvements
- Update of change records and configuration management database
- Closure of change request with appropriate approvals

REVIEW TIMEFRAME: Post-implementation review required but no timeframe specified for completion.

Change Authority Matrix

Change Type	Business Impact	Technical Complexity	Approval Authority
Standard	Low	Low	Technical Lead
Normal - Low Risk	Low	Medium	Change Manager
Normal - Medium Risk	Medium	Medium	Change Advisory Board
Normal - High Risk	High	High	CTO + Security Officer
Emergency	Any	Any	Emergency Change Authority

> **RISK CLASSIFICATION GAP:** Risk levels (Low/Medium/High) referenced in matrix but no criteria provided for determining risk classification.

> **ISO 27001 AUTHORITY GAP:** Authority matrix doesn't address ISO 27001 requirement that changes affecting security controls require security management approval.

Security Change Management

Security-Relevant Changes

Changes affecting information security controls require: - Security impact assessment by qualified security personnel - Review against current threat landscape and risk profile - Validation that security controls remain effective - Update of security documentation and procedures

> **SECURITY QUALIFICATION:** References "qualified security personnel" but no qualifications or certification requirements specified.

Access Control Changes

Changes to user access rights and privileges must: - Follow principle of least privilege - Include business justification for access requirements - Be approved by resource owner and security team - Include regular review and recertification processes

> **CROSS-REFERENCE CONFLICT:** Access control change requirements conflict with Access Control Policy POL-SECU-021 which specifies different approval processes.

Security Control Testing

Changes to security controls require: - Pre-implementation testing in isolated environment - Validation of control effectiveness after implementation - Update of security control documentation - Integration with continuous monitoring processes

> **TESTING ENVIRONMENT:** Requires testing in "isolated environment" but no specification of isolation requirements or test environment standards.

Configuration Management Integration

Configuration Items

Change management covers the following configuration items: - Hardware components and infrastructure - System software and applications - Network devices and configurations - Security controls and monitoring systems - Business processes and procedures

> **CONFIGURATION DEPENDENCY:** References Configuration Management Policy POL-CONFIG-001 which is "under development" creating implementation gaps.

Version Control

- All configuration changes must be version controlled
- Baseline configurations maintained for all critical systems
- Change implementation includes configuration update procedures
- Rollback capabilities require previous configuration preservation

> **VERSION CONTROL SYSTEMS:** Policy requires version control but doesn't specify approved systems or procedures for maintaining version history.

Change Communication

Stakeholder Notification

Change communications must address: - Business users affected by change - Technical teams supporting affected systems - Security and compliance personnel - Senior management for high-impact changes - External parties (clients, vendors) as appropriate

> **COMMUNICATION TIMING:** Stakeholder notification required but no timeframes specified for advance notice or different stakeholder groups.

Communication Channels

- Change advisory board meetings for normal changes
- Email notifications for standard changes
- Emergency communication procedures for urgent changes
- Regular reporting to management on change activities

COMMUNICATION TEMPLATES: References various communication types but no templates or standardised formats provided.

Testing and Validation

Pre-Implementation Testing

- Functional testing to verify change objectives
- Security testing to validate control effectiveness

- Performance testing to ensure system stability
- User acceptance testing for business process changes

TESTING STANDARDS: Various testing types required but no testing standards, methodologies, or acceptance criteria specified.

Rollback Procedures

All changes must include: - Documented rollback procedures tested before implementation - Rollback decision criteria and authority - Time limits for rollback window availability - Data backup and recovery considerations

ROLLBACK AUTHORITY: Rollback decision criteria mentioned but no authority specified for making rollback decisions during implementation.

Emergency Change Management

Emergency Criteria

Emergency changes authorised only when: - Critical system failure affects business operations - Security incident requires immediate remediation - Regulatory compliance deadline cannot be met through normal process - Client contractual obligations at risk of breach

Emergency Procedures

1. Emergency change request initiated with business justification
2. Emergency Change Authority approves change within 2 hours
3. Security team consulted for security-related emergency changes
4. Change implemented with appropriate monitoring and documentation
5. Post-implementation review completed within 48 hours

> **SECURITY CONSULTATION GAP:** Emergency procedure requires security team consultation but no process for after-hours or weekend security team availability.

Post-Emergency Documentation

Emergency changes require: - Formal change request submitted within 24 hours - Root cause analysis of conditions requiring emergency change - Process improvement recommendations - Update of standard procedures to prevent similar emergencies

> **ISO 27001 EMERGENCY GAP:** Emergency procedures lack ISO 27001 A.16.1.5 requirement for "lessons learned from information security incidents" integration with change management.

Change Monitoring and Reporting

Change Metrics

Monthly reporting includes: - Number of changes by category and approval status - Change success rate and failure analysis - Average change implementation time by category - Security impact assessment results - Post-implementation review findings

> **REPORTING AUDIENCE:** Monthly reporting requirements specified but no audience or distribution defined for change management reports.

Compliance Monitoring

- Changes reviewed for regulatory compliance impact
- Audit trail maintained for all change activities
- Regular assessment of change management process effectiveness
- Integration with internal and external audit programs

> **AUDIT INTEGRATION:** References integration with audit programs but no specific requirements or procedures for audit support.

Training and Competency

General Training

All personnel involved in change management receive training on: - Change management policy and procedures - Role-specific responsibilities and authorities - Risk assessment and impact analysis techniques - Documentation and communication requirements

Specialised Training

Key personnel receive additional training on: - Security impact assessment methodologies - Emergency change procedures and decision-making - Change management tools and systems - Regulatory compliance requirements

> **TRAINING EFFECTIVENESS:** Training requirements specified but no competency assessment or effectiveness measurement procedures defined.

Tool and System Requirements

Change Management System

CloudCore uses ServiceNow for change management with requirements for: - Automated workflow and approval routing - Integration with configuration management database - Audit trail and reporting capabilities - Security and access control features

> **SYSTEM INTEGRATION GAP:** References ServiceNow integration with CMDB but Configuration Management Policy under development may conflict with current implementation.

Supporting Tools

- Version control systems for configuration management
- Testing and validation environments
- Monitoring and alerting systems
- Communication and collaboration platforms

> **TOOL STANDARDISATION:** Supporting tools mentioned but no standardisation requirements or approved tool lists provided.

Compliance and Audit

ISO 27001 Compliance

This policy supports ISO 27001:2022 compliance through: - Formal change control procedures (A.12.1.2) - System change control procedures (A.14.2.2) - Management of technical vulnerabilities (A.12.6.1) - Control of operational software (A.12.1.3)

> **INCOMPLETE ISO MAPPING:** Basic ISO control references provided but detailed mapping and evidence requirements not specified.

> **MISSING ISO CONTROLS:** Policy doesn't address relevant ISO 27001 controls: - A.8.1.4 (Information handling in accordance with classification) - A.12.1.1 (Documented operating procedures) - A.14.2.1 (Secure development policy)

Audit Requirements

Change management process subject to: - Annual internal audit of policy compliance - Regular review of change success rates and issues - External audit for regulatory compliance validation - Management review of process effectiveness

> **AUDIT SCOPE GAP:** Audit requirements specified but scope, methodology, and performance criteria not defined.

Record Retention

Change management records retained according to: - Legal and regulatory requirements (minimum 7 years) - Client contractual obligations - Internal audit and compliance needs - Business continuity and disaster recovery requirements

> **RETENTION CONFLICTS:** Retention requirements conflict with Data Classification Policy which specifies different retention periods for operational records.

Exceptions and Waivers

Exception Criteria

Exceptions to change management requirements may be granted when: - Technical limitations prevent standard process compliance - Business urgency requires expedited procedures - Vendor requirements conflict with standard procedures - Regulatory requirements mandate specific approaches

Waiver Process

1. Formal waiver request with business justification
2. Risk assessment and mitigation plan
3. Security team review and approval
4. Time-limited waiver with review requirements
5. Documentation of waiver conditions and monitoring

> **WAIVER AUTHORITY:** Waiver process defined but approval authority not specified for different waiver types and risk levels.

Continuous Improvement

Process Review

Change management process reviewed: - After significant incidents involving changes - Following external audit findings or recommendations - When change success rates fall below targets - As part of annual management system review

> **SUCCESS RATE TARGETS:** References "targets" for change success rates but no specific targets or measurement criteria defined.

Improvement Implementation

Process improvements include: - Updates to policies and procedures based on lessons learned - Tool and system enhancements to support better processes - Training program updates to address identified gaps - Integration improvements with related management systems

> **IMPROVEMENT TRACKING:** Continuous improvement mentioned but no formal process for tracking, prioritising, or implementing improvements.

> **ISO 27001 COMPLIANCE GAPS:** This policy has significant gaps in ISO 27001:2022 compliance: - Incomplete mapping to required controls (A.12.1.2, A.14.2.2) - Missing security impact assessment requirements for all changes - Inadequate documentation of change control procedures - Lack of integration with information security management system - Missing requirements for testing security controls after changes

IMPLEMENTATION CHALLENGES: Policy faces several implementation obstacles: - Dependency on Configuration Management Policy still under development - Undefined Change Advisory Board structure and procedures - Missing change management system integration specifications - Conflicting requirements with other organisational policies - Incomplete role definitions and authority assignments

COMPLIANCE RISK: Current gaps may impact ISO 27001 certification maintenance and regulatory compliance. Priority remediation required for control A.12.1.2 and A.14.2.2 implementation evidence.