SOC 2 Compliance Overview

Document ID: COM-SC-001 **Last Updated:** 2024-02-10 **Owner:** Security & Compliance **Classification:** Internal

---

Introduction

SOC 2 (System and Organization Controls 2) is a framework for managing customer data based on five Trust Service Criteria. This document provides an overview of NovaTech's SOC 2 compliance program.

SOC 2 Basics

What is SOC 2?

SOC 2 is an auditing procedure developed by the AICPA (American Institute of Certified Public Accountants) that ensures service providers securely manage data to protect customer privacy and interests.

Why SOC 2 Matters

- **Customer trust:** Demonstrates commitment to security
- **Competitive advantage:** Required by enterprise customers
- **Risk management:** Structured approach to security
- **Continuous improvement:** Regular audits drive improvements

NovaTech's SOC 2 Status

Aspect	Status
Report Type	SOC 2 Type II
Trust Criteria	Security, Availability, Confidentiality
Audit Period	January 1 - December 31 (annual)
Auditor	[Big Four Firm]
Last Report	January 2024
Next Audit	January 2025

Trust Service Criteria

Security (Common Criteria)

Included in NovaTech's scope

The system is protected against unauthorized access.

Key Controls: - Access control and authentication - Network security - Encryption - Vulnerability management - Security monitoring - Incident response

Availability

Included in NovaTech's scope

The system is available for operation and use.

Key Controls: - Uptime monitoring - Disaster recovery - Business continuity - Capacity planning - Change management

Confidentiality

Included in NovaTech's scope

Information designated as confidential is protected.

Key Controls: - Data classification - Encryption - Access restrictions - Secure disposal - Confidentiality agreements

Processing Integrity

Not currently in scope

System processing is complete, accurate, and authorized.

Privacy

Not currently in scope (covered by separate privacy compliance)

Personal information is collected, used, retained, and disclosed appropriately.

Control Environment

Organizational Structure

```
CEO

    CISO (Security oversight)
         Security Team

    VP Engineering (System controls)
         Platform Team

    VP Legal (Compliance oversight)
          Compliance Team
```

Key Policies

Policy	Document ID	Review Cycle
Information Security Policy	IT-SEC-001	Annual
Access Control Policy	IT-ACC-007	Annual
Change Management Policy	IT-OPS-003	Annual
Incident Response Plan	IT-SEC-020	Annual
Business Continuity Plan	IT-OPS-050	Annual
Vendor Management Policy	COM-VM-001	Annual

Control Categories

CC1: Control Environment

Objective: Demonstrate commitment to integrity and ethical values.

Controls: - Code of conduct - Background checks - Security awareness training - Organizational structure - Board oversight

CC2: Communication and Information

Objective: Support security objectives through communication.

Controls: - Security policies published - Employee training - External communications - Incident reporting channels

CC3: Risk Assessment

Objective: Identify and assess risks to objectives.

Controls: - Annual risk assessment - Threat modeling - Vulnerability assessments - Risk register maintenance

CC4: Monitoring Activities

Objective: Evaluate control effectiveness.

Controls: - Continuous monitoring - Internal audits - Penetration testing - Control testing

CC5: Control Activities

Objective: Deploy controls through policies and procedures.

Controls: - Logical access controls - Physical security - Change management - Vendor management

CC6: Logical and Physical Access

Objective: Restrict system access.

Controls: - User provisioning/deprovisioning - Role-based access control - Multi-factor authentication - Physical access restrictions

CC7: System Operations

Objective: Detect and respond to deviations.

Controls: - Security monitoring - Incident detection - Incident response - Vulnerability management

CC8: Change Management

Objective: Authorize and implement changes properly.

Controls: - Change request process - Testing requirements - Approval workflow - Emergency change process

CC9: Risk Mitigation

Objective: Mitigate risks through controls and insurance.

Controls: - Business continuity planning - Disaster recovery - Cyber insurance - Vendor risk management

---

Evidence Collection

Continuous Evidence

Collected automatically throughout the year: - Access reviews - Change tickets - Security scan results - Training completion - Incident reports

Periodic Evidence

Collected at specific intervals: - Policy reviews (annual) - Risk assessments (annual) - Penetration tests (annual) - BCP tests (annual)

Tools

Tool	Purpose
Vanta	Compliance automation
GitHub	Change management evidence
Okta	Access control evidence
AWS CloudTrail	Audit logs
Datadog	Monitoring evidence

Audit Process

Pre-Audit (Q4)

1. **Gap assessment:** Identify control gaps
2. **Remediation:** Address gaps before audit
3. **Evidence prep:** Organize documentation
4. **Kickoff:** Align with auditors on scope

Audit Period (Full Year)

1. **Walkthrough:** Auditors review controls
2. **Testing:** Sample-based control testing
3. **Inquiry:** Interviews with control owners
4. **Observation:** Direct observation of controls

Post-Audit (Q1 Next Year)

1. **Draft report:** Review auditor findings
2. **Remediation:** Address any exceptions
3. **Final report:** Receive Type II report
4. **Distribution:** Share with customers

Roles and Responsibilities

CISO

- Overall SOC 2 program ownership
- Risk acceptance decisions
- Board reporting

Compliance Team

- Day-to-day program management
- Evidence collection coordination
- Auditor liaison
- Exception tracking

Control Owners

- Maintain assigned controls
- Provide evidence
- Remediate exceptions
- Participate in audits

All Employees

- Follow security policies
- Complete required training

- Report security incidents
- Cooperate with audits

Customer Requests

Obtaining SOC 2 Report

Customers can request our SOC 2 report: 1. Sign NDA (required for report access) 2. Request via customer success or security@novatech.com 3. Receive report within 3 business days

Report Contents

- Auditor's opinion
- Management assertion
- System description
- Trust criteria mapping
- Control descriptions
- Test results
- Any exceptions noted

Bridge Letters

For periods after report date, we provide bridge letters confirming: - No material changes to controls - No significant incidents - Continued compliance

---

Continuous Compliance

Monitoring

- Daily automated control checks
- Weekly compliance dashboard review
- Monthly control owner check-ins
- Quarterly executive review

Improvement

- Track control maturity
- Address audit findings
- Incorporate best practices
- Expand scope as appropriate

Resources

Internal

- Compliance team: compliance@novatech.com
- Compliance portal: [Internal Vanta Link]
- Policy repository: [Internal Notion Link]

External

- AICPA SOC resources
- Trust services criteria (TSC)

Related Documents: Information Security Policy (IT-SEC-001), Risk Assessment Framework (COM-SC-005), Vendor Management Policy (COM-VM-001)