YourIT!
Your Logo Goes Here

Common Controls

Operational Procedures

Prepared for: Client Company

Prepared by: YourIT Company

YourIT!
Your Logo Goes Here

Table of Contents

01 CC1.1 - Inventories

02 CC1.2 - Data Locations

03 CC1.3 - Data Flow Mapping

04 CC1.4 - Data Flow Management

05 CC1.5 - Baseline Configurations

06 CC2.1 - Organization's Supply Chain Role

07 CC2.2 - Organization's Critical Infrastructure Role

08 CC2.3 - Security Official

09 CC2.4 - Workforce Cybersecurity Roles & Responsibilities

10 CC2.5 - Third-Party Cybersecurity Roles & Responsibilities

11 CC2.6 - Workforce Compliance Roles & Responsibilities

12 CC2.7 - Third-Party Compliance Roles & Responsibilities

13 CC2.8 - Roles & Responsibilities Coordination

14 CC2.9 - Agreements

15 CC2.10 - Agreement Compliance Validation

16 CC2.11 - Detection Roles & Responsibilities

17 CC2.12 - Privileged Users

18 CC2.13 - Third-Parties

19 CC2.14 - Senior Executives

20 CC2.15 - Physical Security Personnel

21 CC3.1 - Legal and Regulatory Requirements

22 CC3.2 - Governance & Risk Management Processes

23 CC4.1 - Written Cybersecurity Policies

24 CC4.2 - Written Compliance Policies

25 CC4.3 - Written Procedures

26 CC4.5 - Sanction Policy

27 CC4.6 - Evaluation

28 CC4.7 - System Security Plans (SSP)/Written Information Security Plans (WISP)/Information Security Management System (ISMS)

29 CC4.8 - Security Control Effectiveness

30 CC4.9 - Security Plans of Action

31 CC5.1 - Risk Assessment/Risk Analysis

32 CC5.2 - Prioritize Risks

33 CC5.3 - Risk Management/Mitigation

34 CC5.4 - End-of-Life Products

35 CC5.5 - Monitor Security Controls

36 CC6.1 - Screen Individuals

37 CC6.2 - Terminations & Transfers

38 CC7.1 - Identity Management

39 CC7.2 - Physical Access Management

40 CC7.3 - Remote Access Management

41 CC7.4 - Access Permission Management

42 CC7.5 - Network Segregation

43 CC7.6 - HR Cybersecurity Alignment

44 CC7.7 - Unique User Identification

45 CC7.8 - Identity Authentication

46 CC7.9 - Workforce Authorization & Supervision

47 CC7.10 - Appropriate Access

48 CC7.11 - Access Termination

49 CC7.12 - Limit Access

50 CC7.13 - Limit Functions

51 CC7.14 - Control External Information Systems

52 CC7.15 - Control Publicly Accessible Systems

53 CC7.16 - Identify System Users

54 CC7.17 - Escort & Monitor Visitors

55 CC7.18 - Facility Security Plan

56 CC7.19 - Physical Access Devices

57 CC7.20 - Physical Access Logs

58 CC7.21 - Privacy & Security Notices

59 CC7.22 - Limit Portable Storage Devices

60 CC7.23 - Using Privileged Accounts

61 CC7.24 - Limit Unsuccessful Logons

62 CC7.25 - Authorize Wireless Access

63 CC7.26 - Remote Access Monitoring & Control

64 CC7.27 - Manage Remote Access

65 CC7.29 - Privileged Functions

66 CC7.30 - Terminate Sessions

67 CC7.31 - Wireless Authentication & Encryption

68 CC7.32 - Mobile Device Control

69 CC7.33 - Encrypt Remote Sessions

70 CC7.34 - Authorize Privileged Remote Sessions

71 CC7.35 - Encrypt Mobile Devices

72 CC7.36 - Multifactor Authentication (MFA)

73 CC7.37 - Replay-resistant Authentication

74 CC7.38 - Prevent Identifier Reuse

75 CC7.39 - Disable Identifiers

76 CC8.1 - Protect Data

77 CC8.2 - Manage Assets

78 CC8.3 - Ensure Adequate Capacity

79 CC8.4 - Protect Against Data Leaks

80 CC8.5 - Integrity Checking

81 CC8.6 - Separate Development & Testing Environments

82 CC8.7 - Implement Life Cycle

83 CC8.8 - Change Controls

84 CC8.10 - Data Destruction

85 CC8.11 - Document Data Destruction

86 CC8.13 - Improve Processes

87 CC8.14 - Share Effectiveness Information

88 CC8.15 - Protect & Restrict Removable Media

89 CC8.16 - Control & Limit Access

90 CC8.17 - Anti-Virus/Anti-Malware Protection

91 CC8.18 - Install Patches & Updates

92 CC8.19 - Firewall Protection

93 CC8.20 - Malicious Software Protection & Detection

94 CC8.21 - Monitor Log-in Attempts

95 CC8.22 - Protect Passwords

96 CC8.23 - Data Removal Before Re-use

97 CC8.24 - Disposal

98 CC8.25 - Record Movement

99 CC8.26 - Terminate Sessions

100 CC8.27 - Encrypt Data

101 CC8.28 - Protect Against Alteration or Destruction

102 CC8.29 - Data Integrity

103 CC8.30 - Update Protection

104 CC8.32 - User-installed Software

105 CC8.33 - Security Configurations

106 CC8.34 - Manage Changes

107 CC8.35 - Impact Planning

108 CC8.36 - Minimum Password Complexity

109 CC8.37 - Prohibit Password Reuse

11 CC8.38 - Temporary Passwords

0

111 CC8.39 - Encrypt Passwords

112 CC8.40 - Obscure Authentication Information

113 CC8.41 - Incident Management Process

114 CC8.42 - Scan Files

115 CC8.43 - Monitor Security Alerts

116 CC8.44 - Monitor Systems

117 CC8.45 - Change Security

118 CC8.46 - Restrict Nonessential Resources

119 CC8.47 - Blacklisting

120 CC8.48 - Protect Controlled Unclassified Information (CUI)

121 CC9.1 - Verify Maintenance Personnel

122 CC9.2 - Perform & Control Maintenance & Repairs

123 CC9.3 - Control Maintenance

124 CC9.4 - Manage Remote Maintenance

125 CC9.5 - Third-Party Vendor Compliance

126 CC9.6 - Third-Party Unique User Identification

127 CC9.7 - Remote Maintenance Sessions

128 CC9.8 - Supervise Maintenance Activities

12 CC9.9 - Control Off-site Maintenance

9

130 CC9.10 - Check Diagnostic Programs

131 CC10.1 - Implement Logging/Audit Controls

132 CC10.3 - Review Log Records

133 CC10.4 - Synchronize System Clocks

134 CC10.5 - Logging Failure Alerts

135 CC10.6 - Protect Audit Information

136 CC10.7 - Limit Log Management

137 CC10.8 - Correlate Log Records

138 CC10.9 - Log Reduction & Report Generation

139 CC11.1 - Physical Access Policies

140 CC11.2 - Control Physical Access

141 CC11.3 - Control Physical Security Maintenance

142 CC11.4 - Workstation Physical Security

143 CC11.5 - Restrict Physical Access

144 CC11.6 - Facility Protection & Monitoring

145 CC11.7 - FIPS Encryption

146 CC11.8 - Employ Protection Principles

147 CC11.9 - Limit User Functionality

14 CC11.10 - Prevent

8 Unauthorized/Unintended Data Transfer

149 CC11.11 - Manage Encryption Keys

150 CC11,12 - Control & Monitor Mobile Code

151 CC11.15 - Safeguard Alternate Work Sites

152 CC12.1 - Sanitize Media

153 CC12.2 - Protect Physical Media

154 CC12.3 - Control Removable Media

155 CC12.4 - Mark Media

156 CC12.5 - Control Media Transport

157 CC12.6 - Encrypt Media During Transport

158 CC13.1 - In-transit Data Protection

159 CC13.3 - Encryption of Data in Transit

160 CC13.4 - Transmission Security

161 CC13.5 - Monitor, Control, and Protect Communications

162 CC13.6 - Implement Subnetworks

163 CC13.7 - Protect Communications & Control Networks

164 CC13.8 - Control and Monitor Voice Communications

165 CC13.9 - Authenticity

166 CC13.10 - Deny Network Communications By Default

16 CC13.11 - Prevent Split-Tunneling

7

168 CC13.12 - Terminate Network Connections

169 CC13.13 - Session Lock

170 CC14.1 - Business Continuity & Disaster Recovery Plans

171 CC14.2 - Resource Criticality

172 CC14.3 - Data Criticality

173 CC14.4 - Organizational Priorities

174 CC14.5 - Resource Priorities

175 CC14.6 - Critical Functions

176 CC14.7 - Dependencies

177 CC14.8 - Resliency Requirements

178 CC14.9 - Business Impact Analysis

179 CC14.10 - Likelihood Analysis

180 CC14.11 - Alternative Processes

181 CC14.12 - Data Backup Plan

182 CC14.13 - Backups

183 CC14.15 - Restoration Testing

184 CC14.18 - Recovery Capability Testing

185 CC14.19 - Protect Backups

18 CC15.1 - Remote Activation Prohibition &

6 Use Indicators

187 CC15.2 - Encrypt Network Management Sessions

188 CC16.1 - Workforce Training

189 CC16.2 - Awareness

190 CC16.3 - Track Training

191 CC16.4 - Track Awareness Activities

192 CC16.5 - Insider Threat Training

193 CC17.1 - Vulnerability Scans

194 CC17.2 - Vulnerability Plan

195 CC17.3 - Manage Vulnerabilities

196 CC17.4 - Identify & Report Vulnerabilities

197 CC17.5 - Identify Threats

198 CC17.6 - Threat and Vulnerability Information

199 CC17.7 - Risk Determination

200 CC17.8 - Risk Responses

201 CC17.9 - Risk Management

202 CC17.10 - Risk Tolerance

203 CC17.11 - Risk Tolerance Alignment

204 CC17.12 - Newly-Identified Vulnerabilities

20 CC18.1 - Detect Events

5

206 CC18.2 - Triage Events

207 CC18.3 - Response Procedures

208 CC18.6 - Event Data Correlation

209 CC18.7 - Event Impact Determination

210 CC18.8 - Incident Alert Thresholds

211 CC18.10 - Physical Environment Monitoring

212 CC18.11 - Personnel Activity Monitoring

213 CC18.12 - Malicious Code Detection

214 CC18.13 - Mobile Code Detection

215 CC18.14 - Monitor Service Provider Activity

216 CC18.15 - Monitoring

217 CC18.16 - Detection Compliance

218 CC18.17 - Test Detection Processes

219 CC18.18 - Detection Information Communications

220 CC18.19 - Improve Detection Processes

221 CC19.1 - Incident Response Plan

222 CC19.2 - Test Incident Response Plan

223 CC19.3 - Contain Incidents

22 CC19.4 - Mitigate Incidents

4

225 CC19.5 - Perform Forensics

226 CC19.6 - Categorize Incidents

227 CC19.7 - Understand Incident Impact

228 CC19.8 - Investigate Detection System Notifications

229 CC19.10 - Protect Against Tainting Evidence

230 CC19.11 - Management Notification

231 CC19.12 - Notify Insurance and Attorneys

232 CC19.13 - Follow Incident Response Plan

233 CC19.14 - Personnel Incident Responsibilities

234 CC19.15 - Incident Reporting Determination

235 CC19.16 - Incident Documentation & Reporting

236 CC19.17 - Incident Information Sharing

237 CC19.18 - Victim Notification

238 CC19.19 - Stakeholder Incident Coordination

239 CC19.20 - Stakeholder Information Sharing

240 CC19.21 - Response Plan Lessons Learned

241 CC19.22 - Update Response Strategies

242 CC20.1 - Follow Incident Recovery Plan

24 CC20.2 - Recovery Plan Lessons

3 Learned

244 CC20.3 - Update Recovery Strategies

245 CC20.4 - Manage Public Relations

246 CC20.5 - Reputation Repair

247 CC20.6 - Communicate Recovery Activities

CC1.1 - Inventories

Requirements	Other Requirements
• HIPAA - Security Rule: 164.308(a)(1)(ii)(A) • NIST CSF: ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4	• HIPAA - Security Rule: 164.308(a)(1)(ii)(A) • NIST CSF: ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4 • EU GDPR - Controller and Processor: Article 24(1) • UK GDPR - Controller and Processor: Article 24(1)

Description
Establish and maintain inventories of organizational systems (including hardware, hardware, portable media, mobile devices, industrial control systems, physical security systems, software, cloud services, and firmware) throughout the respective system development life cycles.

Guidance
Automatically or manually identify and locate all hardware, hardware, portable media, mobile devices, industrial control systems, physical security systems, software, cloud services, and firmware. Create reports and update as required.

Procedure
- Use automated tools to identify, locate, and document all PCs, laptops, and servers, including virtual and cloud-based platforms, and identify what data is stored on each.
- Use manual methods, including interviewing users, to identify and locate all PCs, laptops, servers, mobile devices, portable media, cloud services, network devices, printers, and other network-enabled devices, and identify what data is stored on each.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Sanctions/Compliance
Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

CC1.2 - Data Locations

Requirements	Other Requirements
• HIPAA - Security Rule: 164.308(a)(1)(ii)(A) • NIST CSF: ID.AM-3	• HIPAA - Security Rule: 164.308(a)(1)(ii)(A) • NIST CSF: ID.AM-3 • EU GDPR - Controller and Processor: Article 24(1) • UK GDPR - Controller and Processor: Article 24(1)

Description
Locate and identify all organizational data, including data stored on local devices, mobile devices, servers, mass storage, portable media, and cloud platforms.

Guidance
Automatically or manually identify and locate all business data on computers, laptops, servers, storage systems, portable media, cloud services, and mobile devices (smartphones and tablets).

Procedure
- Use automated tools to identify and locate all PCs, laptops, servers, mobile devices, cloud services, network devices, printers, and other network-enabled devices, and identify what data is stored on each.
- Use manual methods, including interviewing users, to identify and locate all PCs, laptops, servers, mobile devices, cloud services, network devices, printers, and other network-enabled devices, and identify what data is stored on each.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Sanctions/Compliance
Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

CC1.3 - Data Flow Mapping

Requirements	Other Requirements
• HIPAA - Security Rule: 164.308(a)(1)(ii)(A) • NIST CSF: ID.AM-3	• HIPAA - Security Rule: 164.308(a)(1)(ii)(A) • NIST CSF: ID.AM-3 • EU GDPR - Controller and Processor: Article 24(1) • UK GDPR - Controller and Processor: Article 24(1)

Description
Create a map of how data flows within and in/out of the organization.

Guidance
Create a map of how data flows within the organization, and in/out of the organization. This needs to cover all business data, and cannot be automated. Mapping data flows requires information from individual departments and users. It is easy to map data flows for organizational systems and platforms shared by all users. It takes questionnaires and interviews to understand how data flows to outside vendors, funding sources, partners, clients, payroll services, consultants, mailing houses, agencies, etc.

Procedure
- Manually work with each department manager and internal Subject Matter Experts to identify how data flows within, and into and out of, the organization, This is often the most critical part of a Business Continuity Business Impact Analysis.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Sanctions/Compliance
Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

CC1.4 - Data Flow Management

Requirements	Other Requirements
• HIPAA - Security Rule: 164.308(a)(1)(ii)(B) • CMMC 2.0 - Level 2: AC.L2-3.1.3	• HIPAA - Security Rule: 164.308(a)(1)(ii)(B) • CMMC 2.0 - Level 2: AC.L2-3.1.3 • NIST 800-171: 3.1.3 • EU GDPR - Controller and Processor: Article 24(1) • UK GDPR - Controller and Processor: Article 24(1)

Description
Ensure that a baseline of network operations and expected data flows for users and systems is established and managed.

Guidance
Data flow management includes the design of networks and storage systems, limiting users to being able to access only the data and resources they need for their jobs. After the initial implementation, it is important to periodically review data flows to ensure unauthorized changes have not been made.

Procedure
- There should be two sets of network diagrams - logical and physical. A logical diagram identifies devices and aligns them to an organizational process or function. A physical diagram identifies the location of each device, including virtual systems and cloud services. All systems must be configured to provide expected data flows and limit access to authorized users only.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Sanctions/Compliance
Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

CC1.5 - Baseline Configurations

Requirements	Other Requirements
• CMMC 2.0 - Level 2: CM.L2-3.4.1 • NIST CSF: PR.IP-1, DE.AE-1	• CMMC 2.0 - Level 2: CM.L2-3.4.1 • NIST 800-171: 3.4.1 • NIST CSF: PR.IP-1, DE.AE-1 • EU GDPR - Controller and Processor: Article 24(1) • UK GDPR - Controller and Processor: Article 24(1)

Description
Establish and maintain baseline configurations of organizational systems (including hardware, portable media, mobile devices, industrial control systems, physical security systems, software, cloud services, firmware, and reporting requirements) throughout the respective system development life cycles.

Guidance
Document approved baseline configurations for all hardware, portable media, mobile devices, industrial control systems, physical security systems, software, cloud services, firmware, and reporting requirements.

Procedure
- Ensure baselines based on all requirements are documented for all PCs, laptops, servers, portable media, mobile devices, industrial control systems, physical security systems, software, cloud services, firmware, and reporting requirements.
- Implement best practice cybersecurity recommendations from manufacturers, government agencies including NIST, and recognized security authorities.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Sanctions/Compliance
Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

CC2.1 - Organization's Supply Chain Role

Requirements	Other Requirements
• NIST CSF: ID.BE-1	• NIST CSF: ID.BE-1

Description
Identify and communicate the organization's role in the supply chain.

Guidance
Identifying your role in the supply chain will help with planning cybersecurity and business continuity programs. Many times organizations play multiple roles in the supply chain, as vendors and service providers and as receivers of products and services required to deliver services.

Procedure
- Define your organization's role in relation to the people you serve, and how your organization is served by others.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Sanctions/Compliance
Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

CC2.2 - Organization's Critical Infrastructure Role

Requirements	Other Requirements
• NIST CSF: ID.BE-2	• NIST CSF: ID.BE-2

Description
Identify and communicate the organization's role in critical infrastructure.

Guidance
Identifying your role in critical infrastrucure will help with planning cybersecurity and business continuity programs. The following business sectors are recognized by the federal government as critical to people's personal safety and everyday life requirements: Chemical Commercial Facilities Communications Critical Infrastructure During COVID-19 Critical Manufacturing Dams Defense Industrial Base Emergency Services Energy Financial Services Food and Agriculture Government Facilities Healthcare and Public Health Information Technology Nuclear Reactors, Materials, and Waste Sector-Specific Agencies Transportation Systems Water and Wastewater Systems

Procedure
- Document your organization's role(s) in one or more of the critical infrastructure categories.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Sanctions/Compliance
Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

CC2.3 - Security Official

Requirements	Other Requirements
• HIPAA - Security Rule: 164.308(a)(2)	• HIPAA - Security Rule: 164.308(a)(2) • EU GDPR - Controller and Processor: Article 37, Article 37(1) • UK GDPR - Controller and Processor: Article 37, Article 37(1)

Description
Identify the security official who is responsible for the development and implementation of the security policies and procedures.

Guidance
This is the individual responsible for evaluating solutions and selecting and implementing those that best meet the organization's requirement. Policies should refer to this person's responsibilty for implementing procedures to support the policies.

Procedure
- Appoint a specific individual to take responsibility for identifying processes and tools that will be used to support the organization's cybersecurity policies.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Sanctions/Compliance
Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

CC2.4 - Workforce Cybersecurity Roles & Responsibilities

Requirements	Other Requirements
• HIPAA - Security Rule: 164.308(a)(3)(ii)(A) • NIST CSF: ID.AM-6	• HIPAA - Security Rule: 164.308(a)(3)(ii)(A) • NIST CSF: ID.AM-6 • EU GDPR - Controller and Processor: Article 39, Article 39(1)(a) • UK GDPR - Controller and Processor: Article 39, Article 39(1)(a)

Description
Establish and document cybersecurity roles and responsibilities within the workforce.

Guidance
All workforce members have cybersecurity responsibilities, from basic users not clicking on malicious links, to data owners responsible for access decisions, to IT responsible for implementing controls, and executives responsible for providing resources and supporting the cybersecurity program.

Procedure
- Work with department heads and Subject Matter Experts to determine the roles of each user, and document how each role should take responsibility for the protection of organizational data. These must align with all compliance requirements.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Sanctions/Compliance
Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

CC2.5 - Third-Party Cybersecurity Roles & Responsibilities

Requirements	Other Requirements
• HIPAA - Security Rule: 164.308(a)(3)(ii)(A)	• HIPAA - Security Rule: 164.308(a)(3)(ii)(A) • EU GDPR - Controller and Processor: Article 32(4), Article 39, Article 39(1)(a) • UK GDPR - Controller and Processor: Article 32(4), Article 39, Article 39(1)(a)

Description
Establish and document cybersecurity roles and responsibilities with third-party stakeholders.

Guidance
Third-parties can refer to vendors, suppliers, software developers, funding sources, clients, etc. It is important to document cybersecurity roles and responsibilities, especially in situations where multiple organizations have shared responsibilities to protect data and comply with requirements.

Procedure
- Work with department heads and Subject Matter Experts to determine the cybersecurity roles of each third-party vendor, and document how each vendor should take responsibility for the protection of organizational data. These must align with all compliance requirements.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Sanctions/Compliance
Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

CC2.6 - Workforce Compliance Roles & Responsibilities

Requirements	Other Requirements
• HIPAA - Security Rule: 164.308(a)(3)(ii)(A)	• HIPAA - Security Rule: 164.308(a)(3)(ii)(A) • EU GDPR - Controller and Processor: Article 39, Article 39(1)(a) • UK GDPR - Controller and Processor: Article 39, Article 39(1)(a)

Description
Establish compliance roles and responsibilities within the workforce.

Guidance
All workforce members have compliance responsibilities, from basic users not violating rules, to data owners responsible for access decisions, to compliance officials ensuring rules are documented and followed, to IT responsible for implementing compliant controls, and executives responsible for providing resources and supporting the compliance program.

Procedure
- Work with department heads and Subject Matter Experts to determine the compliance roles of workforce members, and document how each workforce member should take responsibility for compliance.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Sanctions/Compliance
Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

CC2.7 - Third-Party Compliance Roles & Responsibilities

Requirements	Other Requirements
• HIPAA - Security Rule: 164.308(a)(3)(ii)(A)	• HIPAA - Security Rule: 164.308(a)(3)(ii)(A) • EU GDPR - Controller and Processor: Article 29, Article 32(4), Article 39(1)(a) • UK GDPR - Controller and Processor: Article 29, Article 32(4), Article 39(1)(a)

Description
Establish compliance roles and responsibilities with third-party stakeholders.

Guidance
Third-parties can refer to vendors, suppliers, software developers, funding sources, clients, etc. It is important to document compliance roles and responsibilities, especially in situations where multiple organizations have shared responsibilities to protect data and comply with requirements.

Procedure
- Work with department heads and Subject Matter Experts to determine the compliance roles of each third-party stakeholders, and document how each should take responsibility for compliance.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Sanctions/Compliance
Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

CC2.8 - Roles & Responsibilities Coordination

Requirements	Other Requirements
• NIST CSF: ID.GV-2	• NIST CSF: ID.GV-2 • EU GDPR - Controller and Processor: Article 29, Article 32(4), Article 39(1)(a) • UK GDPR - Controller and Processor: Article 29, Article 32(4), Article 39(1)(a)

Description
Coordinate and align information security roles & responsibilities with internal roles and external partners.

Guidance
There should be formal relationships and defined responsibilities managed through scheduled and responsive activities to ensure security.

Procedure
- Those responsible for information security should interface with department heads, subject matter experts, executives, and third-party stakeholders. Roles should be determined and agreed to prior to incidents to facilitate an orderly response.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Sanctions/Compliance
Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

CC2.9 - Agreements

Requirements	Other Requirements
• HIPAA - Security Rule: 164.308(b)(4)	• HIPAA - Security Rule: 164.308(b)(4) • EU GDPR - Controller and Processor: Article 28(3) • UK GDPR - Controller and Processor: Article 28(3)

Description
Sign agreements that conform with all business and regulatory requirements ensuring third-parties protect data and network access.

Guidance
Agreements may be general confidentiality agreements, or specific agreements tied to regulations, such as HIPAA Business Associate Agreements.

Procedure
- Contracts including cybersecurity requirements should be signed with all third-parties. HIPAA requires Business Associate Agreements using specific language. The NY SHIELD Act requires third-party contracts including cybersecurity requirements.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Sanctions/Compliance
Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

CC2.10 - Agreement Compliance Validation

Requirements	Other Requirements
• HIPAA - Security Rule: 164.308(b)(4)	• HIPAA - Security Rule: 164.308(b)(4) • EU GDPR - Controller and Processor: Article 28(3) • UK GDPR - Controller and Processor: Article 28(3)

Description
Periodically validate that third-parties are living up to their contracted requirements.

Guidance
Signed agreements stored away don't mean anything. It is important to survey third-parties and require evidence they are meeting their contracted requirements.

Procedure
- Questionnaires and site visits can be used to validate third-party adherence to the organization's security requirements.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Sanctions/Compliance
Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

CC2.11 - Detection Roles & Responsibilities

Requirements	Other Requirements
• NIST CSF: DE.DP-1	• NIST CSF: DE.DP-1 • EU GDPR - Controller and Processor: Article 29, Article 32(4), Article 39(1)(a) • UK GDPR - Controller and Processor: Article 29, Article 32(4), Article 39(1)(a)

Description
Ensure that roles and responsibilities for detection are well defined to ensure accountability.

Guidance
Detection responsibilities are critical to ensuring events are identified and evaluated to determine the appropriate response.

Procedure
- Identify roles and assign responsibilities for ensuring detection tools are being used, that alerts are reviewed, and incidents managed according to organizational policies.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Sanctions/Compliance
Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

Truncated Sample Report