Smart Compliance®
Smart Solutions & Services, LLC.
SC365®

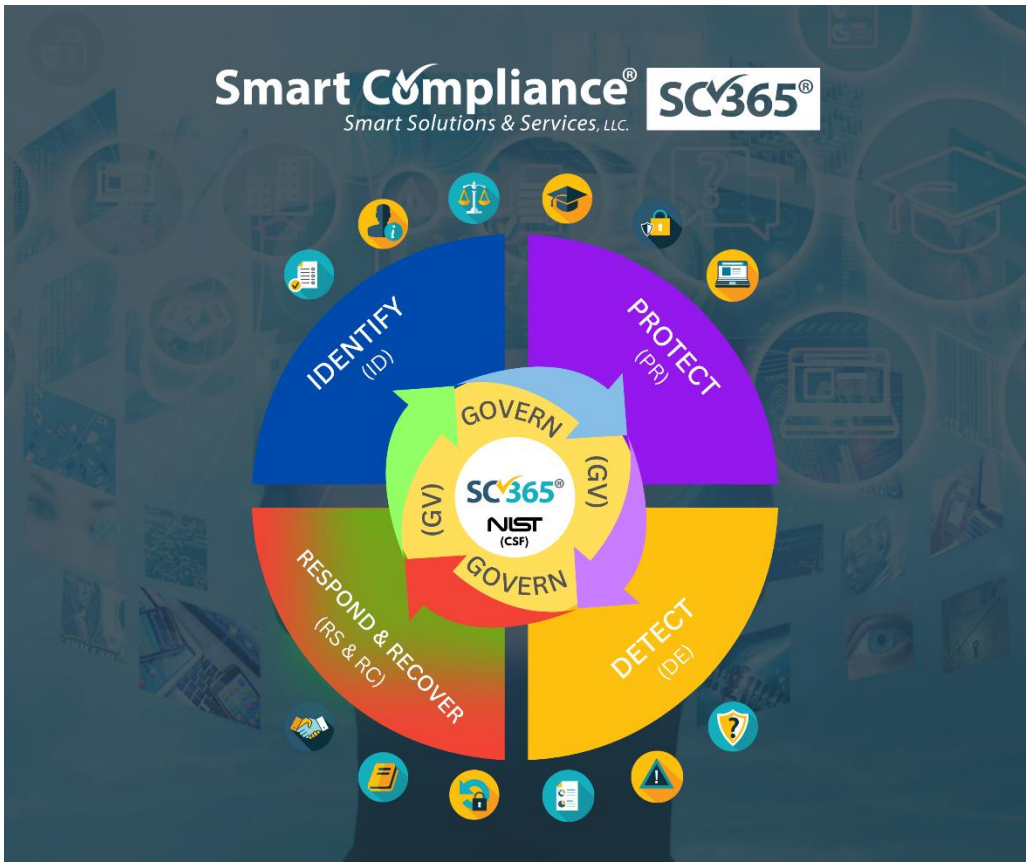
Empower your business cybersecurity with a unique intelligent software solution.

EMPOWERING CYBERSECURITY

SECURITY RULES & NIST CYBERSECURITY FRAMEWORK (CSF) CROSSWALK

Cybersecurity Integrated Solutions

Achieve the benefits of integrating security administrative and technical controls.



Contact us to empower and secure your organization before is too late!

+1(787)620-7575 | info@smartcompliance365.com

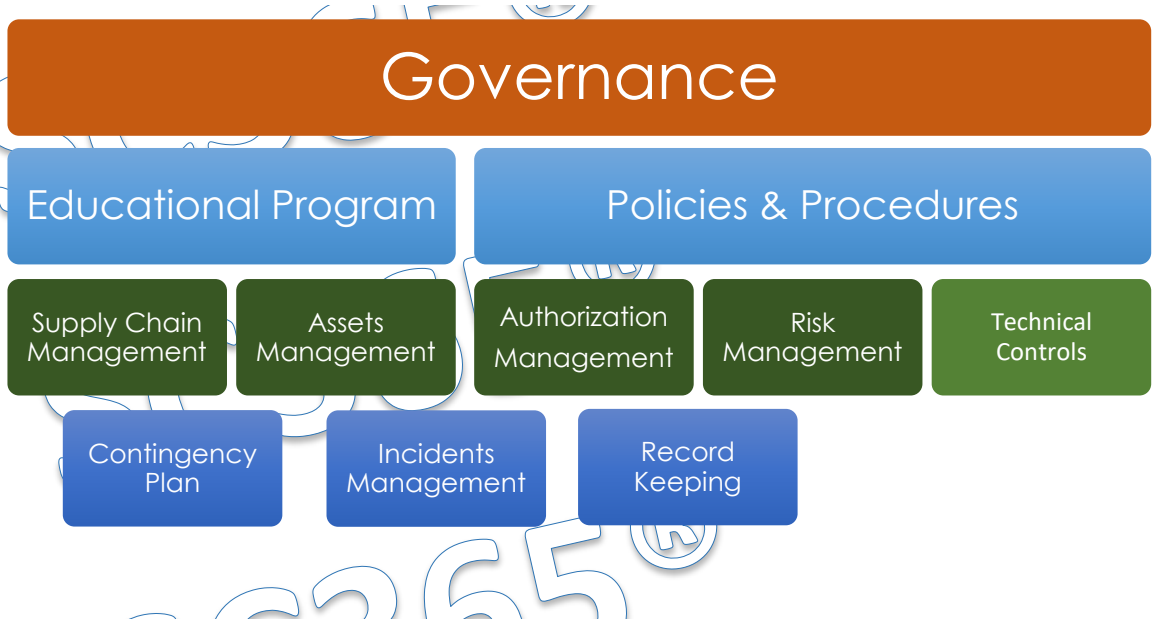
www.smartcompliance365.com

SC365® SOLUTIONS

COMPLIANCE MANAGEMENT | WORKFORCE CLEARANCE | CONTRACTS MANAGEMENT | IT ASSETS | CYBER BI

Cybersecurity Framework

Adopt an effective, robust, and reliable cyber risk management program.



Cyber Insurance Policy

Demonstrate diligence to ensure your cyber insurance coverage.

- **Multifactor authentication for remote access and admin/privileged controls**
- **Endpoint Detection and Response (EDR)**
- **Secured, encrypted, and tested backups**
- **Privileged Access Management (PAM)**
- **Email filtering and web security**
- Patch management and vulnerability management
- Cyber incident response planning and testing
- Cybersecurity awareness training and phishing testing
- Hardening techniques, including Remote Desktop Protocol (RDP) mitigation
- Logging and monitoring/network protections
- End-of-life systems replaced or protected
- Vendor/digital supply chain risk management

Contact us to empower and secure your organization before is too late!

+1(787)620-7575 | info@smartcompliance365.com

www.smartcompliance365.com

SECURITY COMPLIANCE & NIST 2.0 CYBERSECURITY FRAMEWORK		SC365® SOLUTIONS
GOVERN (GV)	**The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.**	
Organizational Context (GV.OC) • ***NIST SP 800-53*** *Rev. 4 CP-2, CP-8, CP-11, PE-9, PE-11, PM-8, PM-8, PM-11, SA-12, SA-14* • ***NIST SP 800-171 (CMMC)*** *Rev. 2:AC 3.1.4; RA 3.11.1, PS 3.9.1; CM 3.4.1* • ***ISO/IEC 27001:2013*** *A.11.1.4, A.11.2.2, A.11.2.3, A.12.1.3, A.15.1.3, A.15.2.1, A.15.2.2, A.17.1.1, A.17.1.2, A.17.2.1* • ***ISA 62443-2-1:2009*** *4.2.2.1, 4.2.3.6* • ***COBIT 5*** *APO02.01, APO02.06, APO03.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05, DSS04.02* • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(4)(ii), 164.308(a)(6)(ii), 164.308(a)(7), 164.308(a)(8), 164.310(a)(2)(i), 164.312(a)(2)(ii), 164.314, 164.316* • ***GDPR*** *Art. 1 (1-3); Art. 3 (1-3) ; Art. 14 (2) (a-g); Art. 28 (1-4); Art. 29; Art. 37 (1-7); Art. 38 (1-6); In. 39 (1-2); Art. 40 (1-11)* • ***GLBA*** *314.4*	**The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood** GV.OC-01: The organizational mission is understood and informs cybersecurity risk management GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated	✓ Compliance ✓ Supply Chain & Contracts
Risk Management Strategy (GV.RM) • ***NIST SP 800-53*** *Rev. 4 CA-2, CA-7, CA-8, PM-4, PM-9, PM-11, PM-12, PM-16, RA-2, RA-3, RA-5, SA-5, SA-11, SA-14, SI-2, SI-4, SI-5* • ***NIST SP 800-171 (CMMC)*** *Rev. 2: CM 3.4.1; SA 3.12.1 – 3.12.4; AT 3.2.1 – 3.2.2* • ***ISO/IEC 27001:2013*** *A.12.6.1, A.18.2.3* • ***ISA 62443-2-1:2009*** *4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12* • ***CCS CSC 4*** • ***COBIT 5*** *APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO13.02, DSS04.02* • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(A), 164.308(a)(6), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.316(a), 164.316(b)(2)(iii), 164.312(c), 164.312(e), 164.314, 164.316* • ***GDPR*** *Art. 28 (1-4); Art. 29; Art. 32 (1-4); Art. 35 (1-6); Articles 77 80; 82-83* • ***GLBA*** *314.4*	**The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions** GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	✓ Compliance ✓ IT Assets ✓ Cyber BI ✓ Workforce ✓ Supply Chain & Contracts ✓ Property

SECURITY COMPLIANCE & NIST 2.0 CYBERSECURITY FRAMEWORK		SC365® SOLUTIONS
GOVERN (GV)	**The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.**	
	GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions	
Roles, Responsibilities, and Authorities (GV.RR) • ***NIST SP 800-53*** *Rev. 4 controls from all families* • ***NIST SP 800-171 (CMMC)*** *Rev. 2: AT 3.2.1, 3.2.3; RA 3.11.1; IR 3.6.2* • ***ISO/IEC 27001:2013*** *A.6.1.1, A.7.2.1, A.18.1* • ***ISA 62443-2-1:2009*** *4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3, 4.4.3.7* • ***COBIT 5*** *APO13.12, DSS04.02, MEA03.01, MEA03.04* • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(2), 164.308(a)(3), 164.308(a)(4), 164.308(b), 164.310, 164.312, 164.314, 164.316* • ***GDPR*** *Art. 6 (1-4) (a); Art. 10 ; Art. 15 (1-4); Art. 28 (1-4); Art. 29; Art. 32 (3-4); Art. 33 (1-5); Art. 34 (1-4); Art. 37 (1-7); Art. 38 (1-6); Art. 39 (1-2); Art. 40 (1-11); Articles 64-66; Articles 84-86* • ***GLBA*** *314.4*	**Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated** GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies GV.RR-04: Cybersecurity is included in human resources practices	✓ Compliance ✓ IT Assets ✓ Workforce ✓ Supply Chain & Contracts
Policy (GV.PO) • ***NIST SP 800-53*** *Rev. 4 controls from all families* • ***NIST SP 800-171 (CMMC)*** *Rev. 2: AT 3.2.1, 3.2.3; RA 3.11.1; IR 3.6.2* • ***ISO/IEC 27001:2013*** *A.6.1.1, A.7.2.1, A.18.1* • ***ISA 62443-2-1:2009*** *4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3, 4.4.3.7* • ***COBIT 5*** *APO13.12, DSS04.02, MEA03.01, MEA03.04* • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(2), 164.308(a)(3), 164.308(a)(4), 164.308(b), 164.310, 164.312, 164.314, 164.316* • ***GDPR*** *Art. 6 (1-4) (a); Art. 10 ; Art. 15 (1-4); Art. 28 (1-4); Art. 29; Art. 32 (3-4); Art. 33 (1-5); Art. 34 (1-4); Art. 37 (1-7); Art. 38 (1-6); Art. 39 (1-2); Art. 40 (1-11); Articles 64-66; Articles 84-86* • ***GLBA*** *314.4*	**Organizational cybersecurity policy is established, communicated, and enforced** GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	✓ Compliance ✓ IT Assets

Oversight (GV.OV) • ***NIST SP 800-53*** *Rev. 4 CA-2, CA-7, CA-8, PM-4, PM-9, PM-11, PM-12, PM-16, RA-2, RA-3, RA-5, SA-5, SA-11, SA-14, SI-2, SI-4, SI-5* • ***NIST SP 800-171 (CMMC)*** *Rev. 2: CM 3.4.1; SA 3.12.1 – 3.12.4; AT 3.2.1 – 3.2.2* • ***ISO/IEC 27001:2013*** *A.12.6.1, A.18.2.3* • ***ISA 62443-2-1:2009*** *4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12* • ***CCS CSC 4*** • ***COBIT 5*** *APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO13.02, DSS04.02* • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(A), 164.308(a)(6), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.316(a), 164.316(b)(2)(iii), 164.312(c), 164.312(e), 164.314, 164.316* • ***GDPR*** *Art. 28 (1-4); Art. 29; Art. 32 (1-4); Art. 35 (1-6); Articles 77 80; 82-83* • ***GLBA*** *314.4*	**Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy** GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	✓ Compliance ✓ IT Assets ✓ Cyber BI ✓ Workforce ✓ Supply Chain & Contracts ✓ Property
Cybersecurity Supply Chain Risk Management (GV.SC) • ***NIST SP 800-53*** *Rev. 4 CP-2, CP-8, CP-11, PE-9, PE-11, PM-8, PM-8, PM-11, SA-12, SA-14* • ***NIST SP 800-171 (CMMC)*** *Rev. 2:AC 3.1.4; RA 3.11.1, PS 3.9.1; CM 3.4.1* • ***ISO/IEC 27001:2013*** *A.11.1.4, A.11.2.2, A.11.2.3, A.12.1.3, A.15.1.3, A.15.2.1, A.15.2.2, A.17.1.1, A.17.1.2, A.17.2.1* • ***ISA 62443-2-1:2009*** *4.2.2.1, 4.2.3.6* • ***COBIT 5*** *APO02.01, APO02.06, APO03.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05, DSS04.02* • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(4)(ii), 164.308(a)(6)(ii), 164.308(a)(7), 164.308(a)(8), 164.310(a)(2)(i), 164.312(a)(2)(ii), 164.314, 164.316* • ***GDPR*** *Art. 1 (1-3); Art. 3 (1-3) ; Art. 14 (2) (a-g); Art. 28 (1-4); Art. 29; Art. 37 (1-7); Art. 38 (1-6); Art. 39 (1-2); Art. 40 (1-11)* • ***GLBA*** *314.4*	**Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders** GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes GV.SC-04: Suppliers are known and prioritized by criticality GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into Supply Chain & Contracts and other types of agreements with suppliers and other relevant third parties GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	✓ Supply Chain & Contracts ✓ Workforce

	GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	

SECURITY COMPLIANCE & NIST 2.0 CYBERSECURITY FRAMEWORK		SC365® SOLUTIONS
IDENTIFY (ID)	**The organization's current cybersecurity risks are understood**	
Asset Management (ID.AM) • ***NIST SP 800-53*** *Rev. 4 CM-8, AC-20, CP-2, RA-2, SA-9, SA-14, PS-7, PM-11* • ***NIST SP 800-171 (CMMC)*** *Rev. 2: CM 3.4.1* • ***ISO/IEC 27001:2013*** *A.6.1.1, A.8.1.1, A.8.1.2, A.8.2.1, A.11.2.6* • ***ISA 62443-2-1****:2009 4.2.3.4, 4.2.3.6, 4.3.2.3.3* • ***ISA 62443-3-3****:2013 SR 7.8* • ***CCS CSC 1, CSC 2*** • ***COBIT 5*** *APO01.02, APO02.02, APO03.03, APO03.04, BAI09.01, BAI09.02, BAI09.05, DSS06.03* • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(2), 164.308(a)(3), 164.308(a)(4), 164.308(a)(7)(ii)(E), 164.308(b), 164.310(a)(2)(ii), 164.310(d) 164.314(a)(1), 164.314(a)(2)(i)(B), 164.314(a)(2)(ii), 164.316(b)(2)* • ***GDPR*** *Articles 35-39;* • ***GLBA*** *314.4*	**Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy** ID.AM-01: Inventories of hardware managed by the organization are maintained ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained ID.AM-04: Inventories of services provided by suppliers are maintained ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles	✓ IT Assets ✓ Cyber BI

Risk Assessment (ID.RA) • ***NIST SP 800-53*** *Rev. 4 CA-2, CA-7, CA-8, PM-4, PM-9, PM-11, PM-12, PM-16, RA-2, RA-3, RA-5, SA-5, SA-11, SA-14, SI-2, SI-4, SI-5* • ***NIST SP 800-171 (CMMC)*** *Rev. 2: CM 3.4.1; SA 3.12.1 – 3.12.4; AT 3.2.1 – 3.2.2* • ***ISO/IEC 27001:2013*** *A.12.6.1, A.18.2.3* • ***ISA 62443-2-1:2009*** *4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12* • ***CCS CSC 4*** • ***COBIT 5*** *APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO13.02, DSS04.02* • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(A), 164.308(a)(6), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.316(a), 164.316(b)(2)(iii), 164.312(c), 164.312(e), 164.314, 164.316* • ***GDPR*** *Art. 28 (1-4); Art. 29; Art. 32 (1-4); Art. 35 (1-6); Articles 77 80; 82-83* • ***GLBA*** *314.4*	**The cybersecurity risk to the organization, assets, and individuals is understood by the organization** ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources ID.RA-03: Internal and external threats to the organization are identified and recorded ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use ID.RA-10: Critical suppliers are assessed prior to acquisition	✓ Compliance ✓ IT Assets ✓ Cyber BI ✓ Supply Chain & Contracts
Improvement (ID.IM) • ***NIST SP 800-53*** *Rev. 4 CP-2, IR-4, IR-8* • ***NIST SP 800-171 (CMMC)*** *Rev. 2: IR 3.6.1,3.6.3* • ***ISO/IEC 27001:2013*** *A.16.1.6* • ***ISA 62443-2-1:2009*** *4.3.4.5.10, 4.4.3.4* • ***COBIT 5*** *BAI01.13* • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.316(b)(2)(iii))* • ***GDPR*** *Art. 32 (1.d) (2)* • ***GLBA*** *314.4*	**Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions** ID.IM-01: Improvements are identified from evaluations ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties ID.IM-03: Improvements are identified from execution of operational processes, procedures, and activities ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	✓ Compliance ✓ IT Assets ✓ Cyber BI

SECURITY COMPLIANCE & NIST 2.0 CYBERSECURITY FRAMEWORK		SC365® SOLUTIONS
PROTECT (PR)	**Safeguards to manage the organization's cybersecurity risks are used**	
Identity Management, Authentication, and Access Control (PR.AA) • ***NIST SP 800-53*** *Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16, AC-17, AC-19, AC-20, PE-2, PE-3, PE-4, PE-5, PE-6, PE-9, IA Family* • ***NIST SP 800-171 (CMMC)*** *Rev. 2: AC 3.1.1, 3.1.2, 3.1.5; CM 3.4.1, 3.4.6; MP 3.8.1-3.8.2, 3.8.5, 3.8.8;PP 3.10.1-3.10.5; PS 3.9.1 – 3.9.2; IA 3.5.1-3.5.2* • ***ISA 62443-2-1:2009*** *4.3.3.3.2, 4.3.3.6.6, 4.3.3.7.3, 4.3.3.3.8, 4.3.3.5.1* • ***ISA 62443-3-3****:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.13, SR 2.1 , SR 2.6* • ***ISO/IEC 27001:2013*** *A.6.1.2, A.6.2.2, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4, A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3, A.13.1.1, A.13.2.1* • ***CCS CSC*** *12, 15, 16* • ***COBIT 5*** *APO13.01, DSS01.04, DSS05.04, DSS06.03, DSS05.05* • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(3), 164.308(a)(4), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.308(b)(1), 164.308(b)(3), 164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d), 164.312(e)(1), 164.312(e)(2)(ii)* • ***GDPR*** *Art. 5 (1) (a-f) ; Art. 25 (1-3); Art. 89 (1-4);* • ***GLBA*** *314.4*	**Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access** PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions PR.AA-03: Users, services, and hardware are authenticated PR.AA-04: Identity assertions are protected, conveyed, and verified PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk	✓ IT Assets ✓ Workforce ✓ Cyber BI ✓ Property
Awareness and Training (PR.AT) • ***NIST SP 800-53*** *Rev. 4 AT-2, AT-3, PM-13, PS-7, SA-9* • ***NIST SP 800-171 (CMMC)*** *Rev. 2: AT 3.2.1 - 3.2.3* • ***ISA 62443-2-1:2009*** *4.3.2.4.2, 4.3.2.4.3* • ***ISO/IEC 27001:2013*** *A.6.1.1, A.7.2.2* • ***COBIT 5*** *APO07.02, APO07.03, APO10.04, APO10.05, BAI05.07, DSS06.03* • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3)(i), 164.308(a)(5), 164.308(b), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii), 164.530(b)(1)* • ***GDPR*** *Art. 28 (1-4); Art. 29; Art. 32 (3-4)* • ***GLBA*** *314.4*	**The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks** PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	✓ Workforce ✓ E-Learning
Data Security (PR.DS) • ***NIST SP 800-53*** *Rev. 4 CM-8, MP-6, PE-16* • ***NIST SP 800-171 (CMMC)*** *Rev. 2: AT 3.2.1; AC 3.1.1, 3.1.2, 3.1.4-3.1.6; CM 3.4.1; MP 3.8.1-3.8.3, 3.8.5, 3.8.8*	**Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information** PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected	✓ IT Assets ✓ Cyber BI

SECURITY COMPLIANCE & NIST 2.0 CYBERSECURITY FRAMEWORK		SC365® SOLUTIONS
PROTECT (PR)	**Safeguards to manage the organization's cybersecurity risks are used**	
• ***ISO/IEC 27001:2013*** *A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7* • ***ISA 62443-2-1:2009*** *4. 4.3.3.3.9, 4.3.4.4.1* • ***ISA 62443-3-3****:2013 SR 4.2* • ***COBIT 5*** *BAI09.03* • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1), 164.310(d)(2)* • ***GDPR*** *Art. 5 (1-2); Art. 32 (1) (a-b); 32(2); Art. 42-44 ; Art. 45 (1-8); Art. 46 (1-5);* • ***GLBA*** *314.4*	PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected PR.DS-11: Backups of data are created, protected, maintained, and tested	
Platform Security (PR.PS) • ***NIST SP 800-53*** *Rev. 4 AU Family, AC-3, AC-4, AC-17, AC-18, CM-7, CP-8, MP-2, MP-4, MP-5, MP-7, SC-7 • CCS CSC 14* • ***NIST SP 800-171 (CMMC)*** *Rev. 2: AC 3.1.1-3.1.2, 3.1.8;* *AT 3.2.1; MP 3.8.4-3.8.6, 3.8.8; SA 3.12.4;* *AA 3.3.3-3.3.7; PP 3.10.4 - 3.10.5;* • ***ISO/IEC 27001:2013*** *A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.1.2, A.11.2.9, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1, A.13.1.1, A.13.2.1* • ***ISA 62443-2-1:2009*** *4.3.3.3.9, 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4* • ***ISA 62443-3-3****:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7, SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6* • ***COBIT 5*** *APO11.04, APO13.01, DSS05.02* • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(C), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iv), 164.312(b)* • ***GDPR*** *Art. 25 (1-3) ; Art. 30 (1-5); Art. 42-44 ; Art. 45 (1-8); Art. 46 (1-5)* • ***GLBA*** *314.4*	**The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability** PR.PS-01: Configuration management practices are established and applied PR.PS-02: Software is maintained, replaced, and removed commensurate with risk PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk PR.PS-04: Log records are generated and made available for continuous monitoring PR.PS-05: Installation and execution of unauthorized software are prevented PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	✓ IT Assets ✓ Cyber BI
Technology Infrastructure Resilience (PR.IR)	**Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience**	✓ IT Assets ✓ Cyber BI

SECURITY COMPLIANCE & NIST 2.0 CYBERSECURITY FRAMEWORK		SC365® SOLUTIONS
PROTECT (PR)	**Safeguards to manage the organization's cybersecurity risks are used**	
• ***NIST SP 800-53*** *Rev. 4 AU Family, AC-3, AC-4, AC-17, AC-18, CM-7, CP-8, MP-2, MP-4, MP-5, MP-7, SC-7* • *CCS CSC 14* • ***NIST SP 800-171 (CMMC)*** *Rev. 2: AC 3.1.1-3.1.2, 3.1.8;* *AT 3.2.1; MP 3.8.4-3.8.6, 3.8.8; SA 3.12.4;* *AA 3.3.3-3.3.7; PP 3.10.4 - 3.10.5;* • ***ISO/IEC 27001:2013*** *A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.1.2, A.11.2.9, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1, A.13.1.1, A.13.2.1* • ***ISA 62443-2-1:2009*** *4.3.3.3.9, 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4* • ***ISA 62443-3-3****:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7, SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6* • ***COBIT 5*** *APO11.04, APO13.01, DSS05.02* • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(C), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iv), 164.312(b)* • ***GDPR*** *Art. 25 (1-3)* **;** *Art. 30 (1-5); Art. 42-44 ; Art. 45 (1-8); Art. 46 (1-5);* • ***GLBA*** *314.4*	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage PR.IR-02: The organization's technology assets are protected from environmental threats PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations PR.IR-04: Adequate resource capacity to ensure availability is maintained	

SECURITY COMPLIANCE & NIST 2.0 CYBERSECURITY FRAMEWORK		SC365® SOLUTIONS
DETECT (DE)	**Possible cybersecurity attacks and compromises are found and analyzed**	
Continuous Monitoring (DE.CM) • ***NIST SP 800-53*** *Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-3, CM-8, CM-10, CM-11, PE-3, PE-6, PE-20, SI-4* • ***NIST SP 800-171 (CMMC)*** *Rev. 2: AA 3.3.3-3.3.6* • ***ISA 62443-3-3****:2013 SR 6.2* • ***ISO/IEC 27001:2013*** *A.12.4.1* • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(a)(2)(i), 164.312(b), 164.312(d), 164.312(e)* • ***GDPR*** *Art. 32 (1.b)* • ***GLBA*** *314.4*	**Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events** DE.CM-01: Networks and network services are monitored to find potentially adverse events DE.CM-02: The physical environment is monitored to find potentially adverse events DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events DE.CM-06: External service provider activities and services are monitored to find potentially adverse events DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	✓ IT Assets ✓ Cyber BI
Adverse Event Analysis (DE.AE) • ***NIST SP 800-53*** *Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, RA-3, SI-4* • ***NIST SP 800-171 (CMMC)*** *Rev. 2: AA 3.3.3-3.3.6; AC 3.1.2-3.2.5* • ***ISA 62443-2-1:2009*** *4.2.3.10* • ***ISA 62443-3-3****:2013 SR 6.1* • ***COBIT 5*** *APO12.06* • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(i), 164.308(a)(6)(ii), 164.308(a)(8), 164.310(d)(2)(iii), 164.312(b), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii)* • ***GDPR*** *Art. 32 (2); Art. 35 (1-2)* • ***GLBA*** *314.4*	**Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents** DE.AE-02: Potentially adverse events are analyzed to better understand associated activities DE.AE-03: Information is correlated from multiple sources DE.AE-04: The estimated impact and scope of adverse events are understood DE.AE-06: Information on adverse events is provided to authorized staff and tools DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria	✓ Compliance ✓ IT Assets ✓ Cyber BI

SECURITY COMPLIANCE & NIST 2.0 CYBERSECURITY FRAMEWORK		SC365® SOLUTIONS
RESPOND (RS)	**Actions regarding a detected cybersecurity incident are taken**	
Incident Management (RS.MA) • ***NIST SP 800-53*** *Rev. 4 CP-2, CP-10, IR-4, IR-8* • ***NIST SP 800-171 (CMMC)*** *Rev. 2: IR 3.6.1-3.6.3* • ***ISO/IEC 27001:2013*** *A.16.1.5* • ***ISA 62443-2-1:2009*** *4.3.4.5.1* • ***COBIT 5*** *BAI01.10* • ***CCS CSC 18*** • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(6)(ii), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.312(a)(2)(ii)* • ***GDPR*** *Art. 32 (1.b); Art. 32 (1.d); Art. 32 (2)* • ***GLBA*** *314.4*	**Responses to detected cybersecurity incidents are managed** RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared RS.MA-02: Incident reports are triaged and validated RS.MA-03: Incidents are categorized and prioritized RS.MA-04: Incidents are escalated or elevated as needed RS.MA-05: The criteria for initiating incident recovery are applied	✓ Compliance ✓ Incident
Incident Analysis (RS.AN) • ***NIST SP 800-53*** *Rev. 4 CP-2, IR-4, IR-5, IR-8* • ***NIST SP 800-171 (CMMC)*** *Rev. 2: IR 3.6.1-3.6.2* • ***ISO/IEC 27001:2013*** *A.16.1.4, A.16.1.6* • ***ISA 62443-2-1:2009*** *4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8* • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(6)(ii), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(E)* • ***GDPR*** *Art. 32 (1.d); Articles 33-34* • ***GLBA 314.4***	**Investigations are conducted to ensure effective response and support forensics and recovery activities** RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident RS.AN-06: Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved RS.AN-08: An incident's magnitude is estimated and validated	✓ Compliance ✓ IT Assets ✓ Cyber BI
Incident Response Reporting and Communication (RS.CO) • ***NIST SP 800-53*** *Rev. 4 CP-2, CP-3, IR-3, IR-8* • ***NIST SP 800-171 (CMMC)*** *Rev. 2: IR 3.6.1-3.6.2* • ***ISO/IEC 27001:2013*** *A.6.1.1, A.16.1.1* • ***ISA 62443-2-1:2009*** *4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4* • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(2), 164.308(a)(6)(i), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.312(a)(2)(ii)* • ***GDPR*** *Articles 33-34; 37-38* • ***GLBA*** *314.4*	**Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies** RS.CO-02: Internal and external stakeholders are notified of incidents RS.CO-03: Information is shared with designated internal and external stakeholders	✓ Compliance ✓ Workforce ✓ Supply Chain & Contracts
Incident Mitigation (RS.MI) • ***NIST SP 800-53*** *Rev. 4 CA-7, RA-3, RA-5* • ***NIST SP 800-171 (CMMC)*** *Rev. 2: IR 3.6.1-3.6.2* • ***ISO/IEC 27001:2013*** *A.12.6.1* • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(6)(ii)* • ***GDPR*** *Art. 32 (1.d); Art. 32 (2); Articles 33-34* • ***GLBA*** *314.4*	**Activities are performed to prevent expansion of an event and mitigate its effects** RS.MI-01: Incidents are contained RS.MI-02: Incidents are eradicated	✓ Compliance ✓ IT Assets ✓ Cyber BI

SECURITY COMPLIANCE & NIST 2.0 CYBERSECURITY FRAMEWORK		SC365® SOLUTIONS
RECOVER (RC)	**Assets and operations affected by a cybersecurity incident are restored**	
Incident Recovery Plan Execution (RC.RP) • ***NIST SP 800-53*** *Rev. 4 CP-10, IR-4, IR-8* • ***NIST SP 800-171 (CMMC)*** *Rev. 2: IR 3.6.1 - 3.6.2; AT 3.2.2* • ***ISO/IEC 27001:2013*** *A.16.1.5* • ***CCS CSC 8*** • ***COBIT 5*** *DSS02.05, DSS03.04* • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(7), 164.310(a)(2)(i)* • ***GDPR*** *Art. 32 (1.c);* • ***GLBA*** *314.4*	**Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents** RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed RC.RP-06: The end of incident recovery is declared based on criteria, and incident- related documentation is completed	✓ Compliance ✓ IT Assets ✓ Supply Chain & Contracts
Incident Recovery Communication (RC.CO) • ***NIST SP 800-53*** *Rev. 4 CP-2, IR-4* • ***NIST SP 800-171 (CMMC)*** *Rev. 2: IR 3.6.1 - 3.6.2* • ***HIPAA Security Rule*** *45 C.F.R. §§ 164.308(a)(6)(ii), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.314(a)(2)(i)(C)* • ***GDPR Art.*** *32 (1.c);* • ***GLBA*** *314.4*	**Restoration activities are coordinated with internal and external parties** RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders RC.CO-04: Public updates on incident recovery are shared using approved methods and messaging	✓ Compliance ✓ Workforce ✓ Supply Chain & Contracts