Policy	Standard #	Standard Title	NIST CSF	FFIEC CAT	FAR 52.204-21	NY DFS 23 NYCRR 500	MA 201 CMR 17.00	OR 646A.622	GLBA
Cybersecurity Governance (GOV)	GOV-1	Publishing Cybersecurity Policies & Standards	ID.GV-1	D1.G.SP.B.4		500.02 500.03	17.03	646A.622(2)(d)	6801(b)(1)
	GOV-2	Periodic Review & Update of Cybersecurity Documentation	ID.GV-1	D1.G.SP.B.4			17.03	646A.622(2)(d)	6801(b)(1)
	GOV-3	Assigned Cybersecurity Responsibilities	ID.AM-6	D1.R.St.B.1 D1.TC.Cu.B.1		500.04	17.03	646A.622(2)(d)	
	GOV-4	Measures of Performance	PR.IP-8	D2.IS.Is.B.1 D2.IS.Is.E.2		500.04			
Asset Management (AST)	AST-1	Asset Governance	ID.AM-1 ID.AM-2 ID.AM-4	D1.G.IT.B.1 D4.RM.Dd.B.2 D4.C.Co.B.3					
	AST-2	Asset Inventories	ID.AM-1 ID.AM-2 ID.AM-4	D1.G.IT.B.1 D4.RM.Dd.B.2 D4.C.Co.B.3					
	AST-3	Assigning Ownership of Assets	ID.AM-1 ID.AM-2 ID.AM-4	D1.G.IT.B.1 D4.RM.Dd.B.2 D4.C.Co.B.3					
	AST-4	Network Diagrams	ID.AM-3	D4.C.Co.B.4 D4.C.Co.Int.1					
	AST-5	Secure Disposal or Re-Use of Equipment	PR.DS-3	D1.G.IT.E.3 D1.G.IT.E.2					
	AST-6	Removal of Assets	PR.DS-3	D1.G.IT.E.3 D1.G.IT.E.2					
	AST-7	Security of Assets Off Premises	PR.DS-1 PR.DS-3	D1.G.IT.B.13 D3.PC.Am.B.14 D4.RM.Co.B.1 D3.PC.Am.A.1 D1.G.IT.E.3 D1.G.IT.E.2					
Business Continuity & Disaster Recovery (BCP)	BCP-1	Contingency Plan	RC.RP-1	D5.IR.Pl.B.6					
	BCP-2	Contingency Training	RC.RP-1	D5.IR.Pl.B.6					
	BCP-3	Contingency Plan Testing & Exercises	RC.RP-1 PR.IP-10	D5.IR.Pl.B.6 D5.IR.Te.B.1 D5.IR.Te.B.3					
	BCP-4	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	RC.IM-1	D5.IR.Pl.Int.4					
	BCP-5	Contingency Plan Update	RC.IM-2	D5.IR.Pl.Int.4 D5.IR.Te.Int.5					
	BCP-6	Information System Recovery & Reconstitution	PR.IP-4	D5.IR.Pl.B.5 D5.IR.Te.E.3					
Capacity & Performance Planning (CAP)	CAP-1	Capacity Management	PR.DS-4						
	CAP-2	Resourcce Priority	PR.DS-4						
Change Management (CHG)	CHG-1	Configuration Change Control	PR.IP-3	D1.G.IT.B.4					
	CHG-2	Security Impact Analysis for Changes	PR.IP-3	D1.G.IT.B.4					
	CHG-3	Security Functionality Verification	PR.IP-3	D1.G.IT.B.4					
Compliance (CPL)	CPL-1	Statutory, Regulatory & Contractual Compliance	ID.GV-3 PR.IP-5	D1.G.Ov.E.2 D3.PC.Am.B.11					6801(b)(3)
	CPL-2	Security Controls Oversight	DE.DP-5 PR.IP-7	D1.RM.RMP.E.2 D1.G.Ov.A.2 D5.IR.Pl.Int.3				646A.622(2)(d)	
	CPL-3	Security Assessments	PR.IP-8	D2.IS.Is.B.1 D2.IS.Is.E.2				646A.622(2)(d)	
Configuration Management (CFG)	CFG-1	System Hardening Through Baseline Configurations	PR.IP-1 PR.IP-3	D3.PC.Im.B.5 D1.G.IT.B.4					
	CFG-2	Least Functionality	PR.IP-1 PR.IP-3	D3.PC.Im.B.5 D1.G.IT.B.4	2	500.07			
	CFG-3	Software Usage Restrictions	PR.IP-1 PR.IP-3	D3.PC.Im.B.5 D1.G.IT.B.4					
Cotinuous Monitoring (MON)	MON-1	Continuous Monitoring	DE.CM-1 DE.DP-1 DE.DP-2 DE.DP-3 DE.DP-4 DE.DP-5 PR.PT-1	D1.G.SP.B.3 D2.MA.Ma.B.1 D2.MA.Ma.B.2 D3.DC.An.B.2 D3.DC.An.B.3 D3.DC.Ev.B.4 D1.G.Ov.E.2 D3.DC.Ev.Int.2 D3.DC.Ev.B.2 D5.ER.Is.B.1 D5.ER.Is.E.1 D5.IR.Pl.Int.3	10	500.06	17.03		
	MON-2	Centralized Event Log Collection	DE.CM-1 DE.DP-2 DE.DP-3 DE.DP-4 DE.DP-5 PR.PT-1	D1.G.SP.B.3 D2.MA.Ma.B.1 D2.MA.Ma.B.2 D3.DC.An.B.2 D3.DC.An.B.3 D1.G.Ov.E.2 D3.DC.Ev.Int.2 D3.DC.Ev.B.2 D5.ER.Is.B.1 D5.ER.Is.E.1 D5.IR.Pl.Int.3		500.06			

Policy	Standard #	Standard Title	NIST CSF	FFIEC CAT	FAR 52.204-21	NY DFS 23 NYCRR 500	MA 201 CMR 17.00	OR 646A.622	GLBA
	MON-3	Content of Audit Records	DE.CM-1 PR.PT-1	D3.DC.An.B.2 D3.DC.An.B.3 D1.G.SP.B.3 D2.MA.Ma.B.1 D2.MA.Ma.B.2		500.06			
	MON-4	Monitoring Reporting	DE.DP-4	D3.DC.Ev.B.2 D5.ER.Is.B.1 D5.ER.Is.E.1		500.06			
	MON-5	Time Stamps	DE.DP-2	D1.G.Ov.E.2		500.06			
	MON-6	Anomalous Behavior	DE.AE-1 DE.CM-3	D3.DC.Ev.B.1 D4.C.Co.B.4 D3.DC.An.A.3		500.06 500.14			
	MON-7	Third-Party Threats	DE.CM-3	D3.DC.An.A.3		500.06			
	MON-8	Privileged Users	DE.CM-6	D4.RM.Om.Int.1		500.06			
	MON-9	Unauthorized Activities	DE.CM-7	D3.DC.Ev.B.3		500.06 500.14			
Cryptographic Protections (CRY)	CRY-1	Use of Cryptographic Protections	PR.DS-1 PR.DS-2 PR.DS-5	D1.G.IT.B.13 D3.PC.Am.B.14 D4.RM.Co.B.1 D3.PC.Am.A.1 D3.PC.Am.B.13 D3.PC.Am.E.5 D3.PC.Am.Int.7 D5.IR.Pl.B.5 D5.IR.Pl.B.6 D5.IR.Pl.E.3 D3.PC.Im.E.4		500.15	17.03		
	CRY-2	Transmission Confidentiality	PR.DS-2	D3.PC.Am.B.13 D3.PC.Am.E.5 D3.PC.Am.Int.7		500.15	17.03		
	CRY-3	Transmission Integrity	PR.DS-8			500.15			
	CRY-4	Encrypting Data At Rest	PR.DS-1	D1.G.IT.B.13 D3.PC.Am.B.14 D4.RM.Co.B.1 D3.PC.Am.A.1		500.15	17.03		
Data Classification & Handling (DCH)	DCH-1	Data Protection	PR.DS-1 PR.DS-2 PR.DS-3	D1.G.IT.B.13 D3.PC.Am.B.14 D4.RM.Co.B.1 D3.PC.Am.A.1 D3.PC.Am.B.13 D3.PC.Am.E.5 D3.PC.Am.Int.7 D1.G.IT.E.3 D1.G.IT.E.2				646A.622(2)(d)	
	DCH-2	Data & Asset Classification	ID.AM-5	D1.G.IT.B.2					
	DCH-3	Media Transportation	PR.DS-3	D1.G.IT.E.3 D1.G.IT.E.2					
	DCH-4	Media Sanitization & Disposal	PR.IP-6		7	500.13		646A.622(2)(d)	
	DCH-5	System Output Handling & Data Retention	PR.IP-6			500.13			
	DCH-6	Removable Media Security	PR.PT-2	D1.G.SP.B.4 D3.PC.De.B.1 D3.PC.Im.E.3					
	DCH-7	Use of External Information Systems	PR.PT-2 PR.PT-3 PR.PT-4	D1.G.SP.B.4 D3.PC.De.B.1 D3.PC.Im.E.3 D3.PC.Am.B.7 D3.PC.Am.B.4 D3.PC.Am.B.3 D4.RM.Om.Int.1 D3.PC.Im.B.1 D3.PC.Am.B.11 D3.PC.Im.Int.1	3				
	DCH-8	Information Sharing	PR.IP-8 PR.PT-2	D2.IS.Is.B.1 D2.IS.Is.E.2 D1.G.SP.B.4 D3.PC.De.B.1 D3.PC.Im.E.3		500.17			
	DCH-9	Publicly Accessible Content	ID.GV-3 ID.GV-4	D1.G.Ov.E.2 D1.G.Ov.B.1 D1.G.Ov.B.3 D1.G.Ov.E.1 D1.G.SP.E.1 D1.G.Ov.Int.1					
	DCH-10	Geographic Location of Data	ID.AM-4	D4.RM.Dd.B.2 D4.C.Co.B.3					
	END-1	Workstation Security	PR.IP-1 DE.CM-4	D3.PC.Im.B.5 D3.DC.Th.B.2					
	END-2	Endpoint Protection Measures	PR.IP-1 DE.CM-4	D3.PC.Im.B.5 D3.DC.Th.B.2					
	END-3	Malicious Code Protection (Antimalware)	DE.CM-4	D3.DC.Th.B.2	13		17.03		
	END-4	Automatic Antimalware Updates	DE.CM-4	D3.DC.Th.B.2	14				

Policy	Standard #	Standard Title	NIST CSF	FFIEC CAT	FAR 52.204-21	NY DFS 23 NYCRR 500	MA 201 CMR 17.00	OR 646A.622	GLBA
Endpoint Security (END)	END-5	Antimalware Always-On Protection	DE.CM-4	D3.DC.Th.B.2	15				
	END-6	File Integrity Monitoring (FIM)	PR.DS-6	D3.PC.Se.Int.3 D3.PC.De.Int.2					
	END-7	Software Firewall	PR.IP-1 DE.CM-4	D3.PC.Im.B.5 D3.DC.Th.B.2			17.03		
	END-8	Phishing & Spam Protection	PR.IP-1 DE.CM-4	D3.PC.Im.B.5 D3.DC.Th.B.2					
	END-9	Mobile Code	DE.CM-5	D3.PC.De.E.5					
Human Resources Security (HRS)	HRS-1	Human Resources Security Management	PR.IP-11	D1.R.St.E.4		500.10	17.03		
	HRS-2	Position Categorization	PR.IP-11 ID.GV-2	D1.G.SP.B.7 D4.RM.Co.B.2 D4.RM.Co.B.5		500.10			
	HRS-3	Users With Elevated Privileges	PR.IP-11	D1.R.St.E.4		500.10			
	HRS-4	Roles & Responsibilities	PR.IP-11 ID.GV-2	D1.G.SP.B.7 D4.RM.Co.B.2 D4.RM.Co.B.5		500.10	17.03		Safeguards Rule
	HRS-5	Personnel Screening	PR.IP-11	D1.R.St.E.4					
	HRS-6	Terms of Employment	PR.IP-11	D1.R.St.E.4	4		17.03		
	HRS-7	Rules of Behavior	PR.IP-11	D1.R.St.E.4			17.03		
	HRS-8	Access Agreements	PR.IP-11	D1.R.St.E.4					
	HRS-9	Personnel Sanctions	PR.IP-11	D1.R.St.E.4			17.03		
	HRS-10	Personnel Transfer	PR.IP-11	D1.R.St.E.4					
	HRS-11	Personel Termination	PR.IP-11	D1.R.St.E.4			17.03		
	HRS-12	Third-Party Personnel Security	PR.IP-11 ID.GV-2	D1.G.SP.B.7 D4.RM.Co.B.2 D4.RM.Co.B.5 D1.R.St.E.4			17.03		
Identification & Authentication (IAC)	IAC-1	Identification & Authentication	PR.AC-1 PR.AC-6	D3.PC.Im.B.7 D3.PC.Am.B.6	5		17.03		
	IAC-2	Multifactor Authentication (MFA)	PR.AC-1 PR.AC-4 PR.AC-6	D3.PC.Im.B.7 D3.PC.Am.B.6 D3.PC.Am.B.1 D3.PC.Am.B.2 D3.PC.Am.B.5		500.12			
	IAC-3	User Provisioning & De-Provisioning	PR.AC-1 PR.AC-4 PR.AC-6	D3.PC.Im.B.7 D3.PC.Am.B.6 D3.PC.Am.B.1 D3.PC.Am.B.2 D3.PC.Am.B.5					
	IAC-4	Role-Based Access Control (RBAC)	PR.AC-1 PR.AC-4 PR.AC-6	D3.PC.Im.B.7 D3.PC.Am.B.6 D3.PC.Am.B.1 D3.PC.Am.B.2 D3.PC.Am.B.5					
	IAC-5	Identifier Management (User Names)	PR.AC-1 PR.AC-4 PR.AC-6	D3.PC.Im.B.7 D3.PC.Am.B.6 D3.PC.Am.B.1 D3.PC.Am.B.2 D3.PC.Am.B.5			17.03		
	IAC-6	Authenticator Management (Passwords)	PR.AC-1 PR.AC-4 PR.AC-6	D3.PC.Im.B.7 D3.PC.Am.B.6 D3.PC.Am.B.1 D3.PC.Am.B.2 D3.PC.Am.B.5	6		17.03		
	IAC-7	Password Authentication Management	PR.AC-1 PR.AC-4 PR.AC-6	D3.PC.Im.B.7 D3.PC.Am.B.6 D3.PC.Am.B.1 D3.PC.Am.B.2 D3.PC.Am.B.5			17.03		
	IAC-8	Account Management	PR.AC-1 PR.AC-4 PR.AC-6	D3.PC.Im.B.7 D3.PC.Am.B.6 D3.PC.Am.B.1 D3.PC.Am.B.2 D3.PC.Am.B.5					
	IAC-9	Periodic Reviews	PR.AC-1 PR.AC-4 PR.AC-6	D3.PC.Im.B.7 D3.PC.Am.B.6 D3.PC.Am.B.1 D3.PC.Am.B.2 D3.PC.Am.B.5					
	IAC-10	Least Privilege	PR.AC-1 PR.AC-4 PR.AC-6	D3.PC.Im.B.7 D3.PC.Am.B.6 D3.PC.Am.B.1 D3.PC.Am.B.2 D3.PC.Am.B.5		500.07	17.03		
	IRO-1	Incident Response Operations	PR.IP-9	D5.IR.Pl.B.1			17.03		

Policy	Standard #	Standard Title	NIST CSF	FFIEC CAT	FAR 52.204-21	NY DFS 23 NYCRR 500	MA 201 CMR 17.00	OR 646A.622	GLBA
Incident Response Operations (IRO)	IRO-2	Incident Handling	DE.AE-2 DE.AE-4 DE.AE-5 RS.AN-1 RS.AN-4 RS.MI-1 RS.MI-2 RS.RP-1	D5.IR.Pl.Int.4 D5.IR.Te.E.1 D5.ER.Es.E.1 D1.RM.RMP.A.4 D5.DR.De.B.1 D3.DC.An.E.4 D3.DC.An.Int.3 D5.IR.Pl.B.1 D5.DR.De.B.3 D5.DR.De.Int.3 D5.ER.Es.B.4 D5.DR.Re.E.1 D5.DR.Re.B.1 D5.DR.Re.E.4 D5.DR.Re.E.2 D5.DR.Re.E.3 D5.DR.De.B.1 D5.DR.Re.E.3 D3.PC.Im.E.4		500.16	17.03		
	IRO-3	Incident Response Plan (IRP)	RS.RP-1 RS.AN-2	D5.IR.Pl.B.1 D1.RM.RMP.A.4 D5.IR.Te.E.1 D5.ER.Es.E.1		500.16	17.03		
	IRO-4	Incident Response Training	RS.RP-1 RS.RP-10	D5.IR.Pl.B.1		500.16			
	IRO-5	Incident Response Testing	RS.RP-1 RS.RP-10 PR.IP-10	D5.IR.Pl.B.1 D5.IR.Te.B.1 D5.IR.Te.B.3		500.16			
	IRO-6	Integrated Incident Response Team	RC.CO-1 RC.CO-2 RC.CO-3 RS.CO-1 RS.CO-4	D5.IR.Pl.B.3 D5.ER.Is.B.1 D5.IR.Pl.Int.1 D5.ER.Es.Int.3		500.16			
	IRO-7	Chain of Custody & Forensics	RS.AN-3	D3.CC.Re.Int.3 D3.CC.Re.Int.4		500.16			
	IRO-8	Incident Monitoring	DE.AE-3	D3.DC.Ev.E.1		500.16	17.03		
	IRO-9	Incident Reporting	RS.CO-2 RS.CO-3 RS.CO-5	D5.IR.Pl.B.2 D5.DR.Re.B.4 D5.DR.Re.E.6 D5.ER.Es.B.4 D5.ER.Es.B.2 D2.IS.Is.B.3 D2.IS.Is.E.2	12	500.16			
	IRO-10	Root Cause Analysis (RCA) & Lessons Learned	RS.IM-1	D5.IR.Pl.Int.4		500.16			
	IRO-11	IRP Update	RS.IM-2	D5.IR.Pl.Int.4 D5.IR.Te.Int.5		500.16			
Maintenance Operations (MNT)	MNT-1	Maintenance Operations	PR.MA-1	D3.CC.Re.Int.5 D3.CC.Re.Int.6					
	MNT-2	Controlled Maintenance	PR.MA-1	D3.CC.Re.Int.5 D3.CC.Re.Int.6					
	MNT-3	Timely Maintenance	PR.MA-1 PR.MA-2	D3.CC.Re.Int.5 D3.CC.Re.Int.6 D3.PC.Im.B.7					
	MNT-4	Remote Maintenance	PR.MA-2	D3.PC.Im.B.7					
Network Security (NET)	NET-1	Layered Defenses	PR.PT-4 PR.AC-5	D3.PC.Im.B.1 D3.PC.Am.B.11 D3.PC.Im.Int.1	11		17.03		
	NET-2	Boundary Protections	PR.AC-5	D3.DC.Im.B.1 D3.DC.Im.Int.1			17.03	646A.622(2)(d)	
	NET-3	Data Flow Enforcement (Access Control Lists)	PR.AC-5	D3.DC.Im.B.1 D3.DC.Im.Int.1					
	NET-4	Information System Connections	PR.AC-5	D3.DC.Im.B.1 D3.DC.Im.Int.1					
	NET-5	Security Function Isolation	PR.AC-5	D3.DC.Im.B.1 D3.DC.Im.Int.1	11				
	NET-6	Virtual Local Area Network (VLAN) Separation	PR.AC-5	D3.DC.Im.B.1 D3.DC.Im.Int.1	11				
	NET-7	Guest Networks	PR.AC-5	D3.DC.Im.B.1 D3.DC.Im.Int.1	11				
	NET-8	Network Disconnect	PR.AC-5	D3.DC.Im.B.1 D3.DC.Im.Int.1					
	NET-9	Network Intrusion Detection & Prevention Systems (NIDS/NIPS)	PR.AC-5	D3.DC.Im.B.1 D3.DC.Im.Int.1	11				
	NET-10	Safeguarding Data Over Open Networks	PR.AC-5	D3.DC.Im.B.1 D3.DC.Im.Int.1					
	NET-11	Remote Access	PR.AC-3	D3.PC.Am.B.15 D3.PC.De.E.7 D3.PC.Im.Int.2					
Physical &	PES-1	Physical & Environmental Protections	PR.IP-5 DE.CM-2	D3.PC.Am.B.11 D3.PC.Am.E.4 D3.Dc.Ev.B.5			17.03	646A.622(2)(d)	
	PES-2	Physical Access Control	PR.AC-2	D3.PC.Am.B.11 D3.PC.Am.B.17	8		17.03		

Policy	Standard #	Standard Title	NIST CSF	FFIEC CAT	FAR 52.204-21	NY DFS 23 NYCRR 500	MA 201 CMR 17.00	OR 646A.622	GLBA
Physical & Environmental Security (PES)	PES-3	Monitoring Physical Access	DE.CM-2						
	PES-4	Visitor Control	DE.CM-2 DE.CM-2		9				
	PES-5	Information Leakage Due To Electromagnetic Signals Emanations	PR.DS-5	D5.IR.Pl.B.5 D5.IR.Pl.B.6 D5.IR.Pl.E.3 D3.PC.Im.E.4					
Project & Resource Management (PRM)	PRM-1	Allocation of Resources	ID.BE-3	D1.G.SP.E.2 D1.G.Ov.Int.5 D1.G.SP.Int.3					
	PRM-2	Security Requirements Definition	ID.BE-3 ID.BE-4 ID.BE-5	D1.G.SP.E.2 D1.G.Ov.Int.5 D1.G.SP.Int.3 D4.C.Co.B.1 D1.G.IT.B.2 D5.IR.Pl.B.5 D5.IR.Pl.E.3					
	PRM-3	Security In Project Management	ID.BE-2 ID.BE-3 ID.BE-4 ID.BE-5	D1.G.SP.Inn.1 D1.G.SP.E.2 D1.G.Ov.Int.5 D1.G.SP.Int.3 D4.C.Co.B.1 D1.G.IT.B.2 D5.IR.Pl.B.5 D5.IR.Pl.E.3					
	PRM-4	System Development Life Cycle (SDLC)	PR.IP-2	D3.PC.Se.B.1 D3.PC.Se.E.1					
Risk Management (RSK)	RSK-1	Risk Management Program (RMP)	ID.GV-4 ID.RM-1 ID.RM-2 ID.RA-3 ID.RA-4 ID.RA-5 ID.RA-6	D1.G.Ov.B.1 D1.G.Ov.B.3 D1.G.Ov.E.1 D1.G.Ov.Int.3 D1.G.SP.E.1 D1.G.Ov.Int.1 D3.DC.An.B.1 D2.MA.Ma.E.1 D2.MA.Ma.E.4 D2.MA.Ma.Int.2 D5.RE.Re.B.1 D5.ER.Er.Ev.1 D1.RM.RA.B.1 D1.RM.RA.E.2 D1.RM.RA.E.1 D5.IR.Pl.B.1 D5.DR.Re.E.1 D5.IR.Pl.E.1		500.09	17.03	646A.622(2)(d)	6801(b)(2)
	RSK-2	Risk Identification	ID.RA-3 ID.RA-4 ID.RA-5 ID.RA-6	D3.DC.An.B.1 D2.MA.Ma.E.1 D2.MA.Ma.E.4 D2.MA.Ma.Int.2 D5.RE.Re.B.1 D5.ER.Er.Ev.1 D1.RM.RA.B.1 D1.RM.RA.E.2 D1.RM.RA.E.1 D5.IR.Pl.B.1 D5.DR.Re.E.1 D5.IR.Pl.E.1		500.09	17.03		Safeguards Rule
	RSK-3	Risk Assessment	ID.RA-3 ID.RA-4 ID.RA-5 ID.RA-6	D3.DC.An.B.1 D2.MA.Ma.E.1 D2.MA.Ma.E.4 D2.MA.Ma.Int.2 D5.RE.Re.B.1 D5.ER.Er.Ev.1 D1.RM.RA.B.1 D1.RM.RA.E.2 D1.RM.RA.E.1 D5.IR.Pl.B.1 D5.DR.Re.E.1 D5.IR.Pl.E.1		500.09	17.03		Safeguards Rule
	RSK-4	Risk Ranking	ID.RA-3 ID.RA-4 ID.RA-5 ID.RA-6 ID.RM-3	D3.DC.An.B.1 D2.MA.Ma.E.1 D2.MA.Ma.E.4 D2.MA.Ma.Int.2 D5.RE.Re.B.1 D5.ER.Er.Ev.1 D1.RM.RA.B.1 D1.RM.RA.E.2 D1.RM.RA.E.1 D5.IR.Pl.B.1 D5.DR.Re.E.1 D5.IR.Pl.E.1 D1.G.SP.A.4		500.09			Safeguards Rule
	RSK-5	Risk Remediation	ID.RA-6	D5.IR.Pl.B.1 D5.DR.Re.E.1 D5.IR.Pl.E.1		500.09		646A.622(2)(d)	Safeguards Rule

Policy	Standard #	Standard Title	NIST CSF	FFIEC CAT	FAR 52.204-21	NY DFS 23 NYCRR 500	MA 201 CMR 17.00	OR 646A.622	GLBA
	RSK-6	Business Impact Assessments (BIAs)	ID.RA-4 ID.RA-5 ID.RM-3	D5.RE.Re.B.1 D5.ER.Er.Ev.1 D1.RM.RA.B.1 D1.RM.RA.E.2 D1.RM.RA.E.1 D1.G.SP.A.4		500.09			Safeguards Rule
Secure Engineering & Architecture (SEA)	SEA-1	Security Engineering Principles	PR.AC-4 PR.IP-1 PR.PT-2	D3.PC.Im.B.5 D1.G.SP.B.4 D3.PC.De.B.1 D3.PC.Im.E.3			17.03	646A.622(2)(d)	
	SEA-2	Secure Configurations	PR.IP-1	D3.PC.Im.B.5			17.03		
	SEA-3	Least Functionality	PR.PT-3	D3.PC.Am.B.7 D3.PC.Am.B.4 D3.PC.Am.B.3 D4.RM.Om.Int.1			17.03		
	SEA-4	Fail Secure In Known State	PR.PT-5						
	SEA-5	Clock Synchronization	PR.IP-1	D3.PC.Im.B.5					
Operations Security (OPS)	OPS-1	Operations Security	ID.GV-2 RS.CO-1	D1.G.SP.B.7 D4.RM.Co.B.2 D4.RM.Co.B.5 D5.IR.Pl.B.3					
	OPS-2	Standardized Operating Procedures (SOPs)	ID.GV-2 RS.CO-1	D1.G.SP.B.7 D4.RM.Co.B.2 D4.RM.Co.B.5 D5.IR.Pl.B.3					
Security Awareness & Training (SAT)	SAT-1	Security-Minded Workforce	PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5	D1.TC.Tr.B.2 D1.TC.Tr.E.3 D1.TC.Tr.B.4 D1.TC.Tr.Int.2 D1.TC.Tr.E.2 D1.TC.Tr.E.3 D1.R.St.E.3		500.10 500.14	17.03	646A.622(2)(d)	
	SAT-2	Security Awareness	PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5	D1.TC.Tr.B.2 D1.TC.Tr.E.3 D1.TC.Tr.B.4 D1.TC.Tr.Int.2 D1.TC.Tr.E.2 D1.TC.Tr.E.3 D1.R.St.E.3		500.10 500.14	17.03		
	SAT-3	Security Training	PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5	D1.TC.Tr.B.2 D1.TC.Tr.E.3 D1.TC.Tr.B.4 D1.TC.Tr.Int.2 D1.TC.Tr.E.2 D1.TC.Tr.E.3 D1.R.St.E.3		500.10 500.14	17.03	646A.622(2)(d)	
	SAT-4	Security Training Records	PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5	D1.TC.Tr.B.2 D1.TC.Tr.E.3 D1.TC.Tr.B.4 D1.TC.Tr.Int.2 D1.TC.Tr.E.2 D1.TC.Tr.E.3 D1.R.St.E.3		500.10 500.14			
Technology Development & Acquisition (TDA)	TDA-1	Technology Development & Acquisition	PR.IP-1 PR.DS-7	D3.PC.Im.B.5 D3.PC.Am.B.10		500.08		646A.622(2)(d)	
	TDA-2	Security Requirements	PR.IP-1 PR.DS-7	D3.PC.Im.B.5 D3.PC.Am.B.10		500.08			
	TDA-3	Design & Implementation of Security Controls	PR.IP-1 PR.DS-7	D3.PC.Im.B.5 D3.PC.Am.B.10		500.08			
	TDA-4	Functional Properties of Security Controls	PR.IP-1 PR.DS-7	D3.PC.Im.B.5 D3.PC.Am.B.10		500.08			
	TDA-5	Secure Development	PR.IP-1 PR.DS-7	D3.PC.Im.B.5 D3.PC.Am.B.10		500.08		646A.622(2)(d)	
	TDA-6	Secure Development Environments	PR.IP-1 PR.DS-7	D3.PC.Im.B.5 D3.PC.Am.B.10		500.08			
	TDA-7	Separation of Development, Testing and Operational Environments	PR.IP-1 PR.DS-7	D3.PC.Im.B.5 D3.PC.Am.B.10		500.08			
	TDA-8	Security Testing Throughout Development	PR.IP-1 PR.DS-7	D3.PC.Im.B.5 D3.PC.Am.B.10		500.08			
Third-Party Management (TPM)	TPM-1	Third-Party Management	ID.SC-1			500.11	17.03		
	TPM-2	Third-Party Criticality Assessments	ID.BE-1 ID.SC-2	D1.G.SP.A.3		500.11			
	TPM-3	Supply Chain Protection	ID.SC-4			500.11	17.03		
	TPM-4	Third-Party Services	ID.SC-1 ID.SC-2 ID.SC-3 ID.SC-4 ID.SC-5			500.11			
	TPM-5	Written Contract Requirements	ID.SC-3			500.11	17.03		
	TPM-6	Review of Third-Party Services	ID.SC-4			500.11	17.03		
	TPM-7	Third-Party Deficiency Remediation	ID.SC-4			500.11			

Policy	Standard #	Standard Title	NIST CSF	FFIEC CAT	FAR 52.204-21	NY DFS 23 NYCRR 500	MA 201 CMR 17.00	OR 646A.622	GLBA
	TPM-8	Managing Changes To Third-Party Services	ID.SC-4			500.11			
	TPM-9	Third Party Incident Response & Recovery Capabilities	ID.SC-5			500.11			
Threat Management (THR)	THR-1	Threat Awareness Program	ID.BE-2	D1.G.SP.Inn.1		500.10			
	THR-2	Threat Intelligence Feeds	ID.RA-2	D2.TI.Ti.B.1		500.10			
Vulnerability & Patch Management (VPM)	VPM-1	Vulnerability & Patch Management Program (VPMP)	ID.RA-1 PR.IP-12	D2.TI.Ti.B.2 D3.DC.Th.B.1 D1.RM.RA.E.2 D3.DC.Th.E.5 D3.DC.Th.A.1 D3.CC.Re.Ev.2					
	VPM-2	Vulnerability Ranking	ID.RA-1 PR.IP-12	D2.TI.Ti.B.2 D3.DC.Th.B.1 D1.RM.RA.E.2 D3.DC.Th.E.5 D3.DC.Th.A.1 D3.CC.Re.Ev.2					
	VPM-3	Vulnerability Remediation	ID.RA-1 PR.IP-12 RS.MI-3	D2.TI.Ti.B.2 D3.DC.Th.B.1 D1.RM.RA.E.2 D3.DC.Th.E.5 D3.DC.Th.A.1 D3.CC.Re.Ev.2 D1.RM.RA.E.1					
	VPM-4	Software Patching	PR.IP-12 RS.MI-3	D3.CC.Re.Ev.2 D1.RM.RA.E.1					
	VPM-5	Vulnerability Scanning	DE.CM-8	D3.DC.Th.E.5					
	VPM-6	Penetration Testing	DE.CM-8	D3.DC.Th.E.5		500.05			
	VPM-7	Red Team Exercises	DE.DP-3	D3.DC.Ev.Int.2					
Web Security (WEB)	WEB-1	Use of Demilitarized Zones (DMZs)	PR.AC-4 PR.AC-5	D3.PC.Am.B.1 D3.PC.Am.B.2 D3.PC.Am.B.5 D3.DC.Im.B.1 D3.DC.Im.Int.1					
	WEB-2	Cloud Providers	PR.AC-4 PR.AC-5	D3.PC.Am.B.1 D3.PC.Am.B.2 D3.PC.Am.B.5 D3.DC.Im.B.1 D3.DC.Im.Int.1	4				
	WEB-3	Cloud Security Architecture	PR.AC-4 PR.AC-5	D3.PC.Am.B.1 D3.PC.Am.B.2 D3.PC.Am.B.5 D3.DC.Im.B.1 D3.DC.Im.Int.1	4				
	WEB-4	Security Management Subnet	PR.AC-4 PR.AC-5	D3.PC.Am.B.1 D3.PC.Am.B.2 D3.PC.Am.B.5 D3.DC.Im.B.1 D3.DC.Im.Int.1	4				
	WEB-5	Multi-Tenant Environments	PR.AC-4 PR.AC-5	D3.PC.Am.B.1 D3.PC.Am.B.2 D3.PC.Am.B.5 D3.DC.Im.B.1 D3.DC.Im.Int.1	4				
	WEB-6	Geolocation Requirements	PR.AC-4 PR.AC-5	D3.PC.Am.B.1 D3.PC.Am.B.2 D3.PC.Am.B.5 D3.DC.Im.B.1 D3.DC.Im.Int.1	4				
	WEB-7	Sensitive Data In Public Cloud Providers	PR.AC-4 PR.AC-5	D3.PC.Am.B.1 D3.PC.Am.B.2 D3.PC.Am.B.5 D3.DC.Im.B.1 D3.DC.Im.Int.1	4				