BeachheadSecure® Compliance Controls

About this chart:
Chart is organized following the categories delineated in the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond and Recover). Identified are the functions provided BeachheadSecure and the controls it satisfies of CMMC Levels 1 & 2, ISO 27001, NIST Cybersecurity Framework and FTC Safeguards.

IDENTIFY

Categories	BeachheadSecure Function	Compliance Standard Controls				
		CMMC Level 1	CMMC Level 2	ISO 27001	NIST CSF	FTC Title 16
Asset Management: Inventory of Assets	BeachheadSecure enables remote identification and management of organization's devices		CM.L2-3.4.1	A.8.1.1	ID-AM-1	Section 314(b)
Risk Assessment: Understanding, identifying and documenting cybersecurity risks to organizaiton	BeachheadSecure's RiskResponder meaures, documents and responds to cyberrisks		RA.L2-3.11.1	A.16.1.2,A.16.1.3	ID.RA-1, ID.RA.3, ID.RA.4, ID.RA-5, ID.RA-6	

PROTECT

Categories	BeachheadSecure Function	Compliance Standard Controls				
		CMMC Level 1	CMMC Level 2	ISO 27001	NIST CSF	FTC Title 16
Access Controls: Limit and/or protect access to organization's decices and systems	RiskResponder - invalid login attempts	SC.L1-3.1+A15:A233.1+C12:F24	AC.L2-3.1.8	A.9.1.2, A.9.2.3, A.9.2.6, A.9.4.1, A.9.4.2, A.9.4.5, A.12.4.2		
	MFA -Multifactor Authentication	IA.L1-3.5.2	IA.L2-3.5.3		PR.AC-6	Section 314.(c) (1)(i) Section 314.(c) (5)
	Session control	AC.L1-3.1.1	AC.L2-3.1.11			
	Management of access controls (misc)		AC.L2-3.1.12		PR.AC-1, PR.AC-3, PR.C-4, PR.AC-6, PR.AC-7	Section 314.(c) (1)(i)
Data Security: Secure management and protection of organization's data	System- & user-level layered encryption -- protecting data at rest		AC.L2-3.1.19,SC.L2-3.13.11,SC.L2-3.13.16	A.10.1.1, A.10.2, A.14.2.2, A.14.3.1	PR-DS-1	Section 314.(c) (3)
	Data destruction, data quarrantine, data sanitization	MP.2.121	MP.1.118, MP.L1-3.8.3	A.8.3.2, A.11.2.7	PR.D-3	Section 314.(c) (6)(i)
	Protection against data exfiltration (user-level encryption and management of Windows Security Controled Folders)	MP.2.121			PR.DS-5	
	RiskResponder -- protection against data leakage/exfiltraiton through geofencing controls	SC.L1-3.13.1	AC.L2-3.1.19,SC.L2-3.13.11	A.11.1.2,A-12.2.5	PR-DS-4	
	Protection of removable media data, and protecting against unauthorized use of removable media	MP.2.121	MP.L2-3.8.6,MP.L2-3.8.7, MP.L2-3.8.8,AC.L2-3.1.21	A.8.3.1	PR.PT-2	
	protect and encrypt data on mobile devices		AC.L2-3.1.19	A.6.2.1	PR.DS-1	Section 324.(c)(3)
	RiskResponder protects against invalid logon attempts		AC.L2-3.1.8	A.11.1.4	PR.DS-4, PR.DS-5	
Protective Technology -- Technical security solutions are managed to ensure security and resiliance of systems and assets	Audit & logging capabilities	AU.3.045	AU.3.045,AU.L2-3.3.3, IR.3.098, IR.L2-3.6.2	A.12.4.1, A.12.4.3	PR.PT-1	

BeachheadSecure® Compliance Controls

About this chart:
Chart is organized following the categories delineated in the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond and Recover). Identified are the functions provided BeachheadSecure and the controls it satisfies of CMMC Levels 1 & 2, ISO 27001, NIST Cybersecurity Framework and FTC Safeguards.

DETECT

Categories	BeachheadSecure Function	Compliance Standard Controls				
		CMMC Level 1	CMMC Level 2	ISO 27001	NIST CSF	FTC Title 16
Asset Management: Secure management of data and stytems	BeachheadSecure multifactor authentication- management of secure access controls	IA.L1-3.5.2	IA.L2-3.5.3	A.9.1.2, A.9.2.3, A.9.2.6, A.9.4.1, A.9.4.2, A.9.4.5, A.12.4.2	DE.AE-1	Section 314(b)
	BeachheadSecure -- analysis and reporting of security events	IA.L1-3.5.2	IR.L2-3.6.2	A.12.4.1	DE.AE-2, DE.AE-3	
Continuous Monitoring: Monitoring for vulnerabalities to systems and data	BeachheadSecure's management of Windows Security and RiskResponder -- continuous monitoring of for potential cybersecurity events and malicious code	SI.L1-3.14.2,SI.L1-3.14.5	RA.L2-3.11.2, SI.L2-3.14.6	A.12.2.1	DE.CM-1, DE-CM-2, DE-CM-3, DE.CM-4	

RESPOND

Categories	BeachheadSecure Function	Compliance Standard Controls				
		CMMC Level 1	CMMC Level 2	ISO 27001	NIST CSF	FTC Title 16
Response Procedures and Policies are implemented: Ensuring response to cybersecurity event	Logging and reporting (including Compliancy Report) capability assists in responding to incidents, and facilitates organization awareness of threats	AU.3.045	AU.L2-3.3.3, IR.3.098, IR.L2-3.6.2	A.12.4.1, A.12.4.3,A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.7	RS.RP-1, RS.CO-2, RS.CO-3, RS.CO-5	Section 314(b)
Analysis is Conducted: Ensure effective response and support recovery activities	Logging and reporting (including Compliancy Report) capability assists in the analysis of cyberthreats, and with the implementation of recovery activities	AU.3.045	AU.L2-3.3.3, IR.3.098, IR.L2-3.6.2	A.12.4.1, A.12.4.3,A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.7	RS.AN-1, RS.AN-2, RS.AN-3,RS.AN-4	

RECOVER

Categories	BeachheadSecure Function	Compliance Standard Controls				
		CMMC Level 1	CMMC Level 2	ISO 27001	NIST CSF	FTC Title 16
Recovery processes and planning are improved by incorporating lessons learned	Logging and reporting capability assists identifying vulnerabilites and risks as a part of the recovery process		IR.L2-3.6.1, IR.L2-3.6.2	A.18.2.2	RC.IM-1	Section 314(b)