anchor@anchor-cyber:~$ man csf-for-smb

ANCHOR CYBER SECURITY LLC

CSF 2.0 for Small Business

Based on NIST SP 1300 — for a client with no security program yet, or Anchor's own quick first-conversation checklist. Every action below cites the real Subcategory it comes from.

SP 1300 doesn't give you all 106 Subcategories — it hand-picks the highest-leverage action per Function under four verbs: **Understand** it, **Assess** it, **Prioritize** it, **Communicate** it. That's the order that actually works for a business with no plan today, not the order NIST lists the Functions in.

$ csf-smb --govern

GOVERN Set the strategy and who's accountable for it

UNDERSTAND	How a breach would actually disrupt your mission	GV.OC-01
	Your real legal, regulatory, contractual obligations	GV.OC-03
	Who owns building and running the security plan	GV.RR-02
ASSESS	Impact if you lost critical assets or ops entirely	GV.OC-04
	Whether cyber insurance makes sense for you	GV.RM-04
	Supplier risk before signing, not after	GV.SC-06
PRIORITIZE	Cyber risk sits next to your other business risks — not in its own silo	GV.RM-03
COMMUNICATE	Leadership visibly backs a risk-aware culture	GV.RR-01
	Policies get enforced, not just written	GV.PO-01

$ csf-smb --identify

IDENTIFY Know what you actually have before you protect it

UNDERSTAND	A real inventory of hardware, software, systems, services	ID.AM-01/02/04
ASSESS	Where the vulnerabilities in that inventory actually are	ID.RA-01
	How well your program is actually working	ID.IM-01
PRIORITIZE	Classify data by sensitivity — not everything is equally critical	ID.AM-07
	Keep a risk register, not tribal knowledge	ID.RA
COMMUNICATE	Plans and best practices reach staff and relevant third parties	ID.IM-04

$ csf-smb --protect

PROTECT The Function with the cheapest, fastest wins

UNDERSTAND	Restrict sensitive access to only who needs it for their job	PR.AA-05
ASSESS	Whether staff training is timely, current, and actually happening	PR.AT-01/02
PRIORITIZE	MFA on every account that offers it — the single fastest win here	PR.AA-03
	Change every default manufacturer password	PR.AA-01
	Auto-update and patch; don't rely on remembering	PR.PS-02
	Back up data and actually test the restore	PR.DS-11
	Full-disk encryption on laptops and tablets	PR.DS-01
COMMUNICATE	Staff can recognize and report an attack, and do basic cyber hygiene	PR.AT-01/02

$ csf-smb --protect --mfa-check

NIST's own starter list — yours will be longer, but if these seven aren't covered, nothing else here matters yet.

ACCOUNT	MFA ENABLED?
Banking account(s)	_____
Accounting / tax account(s)	_____
Merchant account(s)	_____
Google / Microsoft / Apple ID account(s)	_____
Email account(s)	_____
Password manager	_____
Primary website account	_____

$ csf-smb --detect

DETECT Find it before a customer or the news tells you

UNDERSTAND	What a cybersecurity incident actually looks like day to day `DE.CM`
ASSESS	Deviations from normal in your tech and external services `DE.CM-06/09`
	Physical tampering or suspicious activity on-site `DE.CM-02`
PRIORITIZE	Antivirus/anti-malware on every business device — including personal devices touching business data `DE.CM-09`
	A monitoring provider if you don't have staff to watch this yourselves `DE.CM`
COMMUNICATE	Give your incident responder the actual details, not a summary `DE.AE-06/07`

$ csf-smb --respond

RESPOND What you do in the first hour matters more than the plan looks

UNDERSTAND	Who has authority to act on the incident response plan `RS.MA-01`
ASSESS	Your actual ability to respond, not your intended one `RS.MA-01`
	Severity and root cause, before you decide what's next `RS.AN-03, RS.MA-03`
PRIORITIZE	Contain and eradicate before anything else, including PR `RS.MI`
COMMUNICATE	Confirmed incidents to stakeholders as law, contract, or policy requires — not "when it's convenient" `RS.CO-02/03`

$ csf-smb --respond --who-to-call

Fill this in before you need it. An incident is the worst possible time to be looking up a phone number.

CONTACT	PHONE
Business leader	_____
Technical contact	_____
State police / local law enforcement	_____
Legal counsel	_____
Bank	_____
Cyber insurance carrier	_____

$ csf-smb --recover

RECOVER

Get back to normal without reintroducing the same hole

UNDERSTAND	Who inside and outside the business owns recovery	RC.RP-01
ASSESS	Write the after-action report while it's still fresh	RC.RP-06
	Verify backup integrity before you restore from it	RC.RP-03
PRIORITIZE	Recovery order by organizational need, resources, and actual impact	RC.RP-02
COMMUNICATE	Regular updates to stakeholders during recovery	RC.CO
	Document when the incident is actually closed	RC.RP-06

src: NIST SP 1300, CSF 2.0 Small Business Quick-Start Guide (Feb 2024) exit 0