Cyber Risk Frameworks to Secure Your Business

because “best practices” doesn’t mean anything…

NIST CSF → Great starting point, especially for SMBs flexible, risk-based.	https://www.nist.gov/cyberframework
NIST 800-53 → Deep control catalog best for complex orgs & risk based	https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
NIST 800-171 → Required for U.S. DoD contractors w/ CUI	https://csrc.nist.gov/pubs/sp/800/171/a/r3/final
CMMC → U.S. defense contractors; maturity model layered on 800-171.	https://dodcio.defense.gov/CMMC
FISMA → Federal agencies and contractors; requires risk-based program.	https://csrc.nist.gov/projects/risk-management/fisma-background
PCI DSS → Anyone handling payment cards	https://www.pcisecuritystandards.org
SOC 2 → SaaS, cloud, and service providers; trust assurance for clients.	https://www.aicpa.org/soc4so
ISO 27001 → International standard, structured and certifiable	https://www.iso.org/isoiec-27001-information-security.html
ISO 27701 → Add-on to 27001 for privacy management.	https://www.iso.org/standard/71670.html
ISO 22301 → Business continuity often required in critical industries.	https://www.iso.org/standard/75106.html
CIS Controls → Lightweight, practical, great for SMBs and quick wins.	https://www.cisecurity.org/controls
CSA STAR / CCM → Cloud providers, especially SaaS/IaaS needing assurance.	https://cloudsecurityalliance.org/star
COBIT → IT governance + management framework	https://www.isaca.org/resources/cobit
HITRUST CSF → Healthcare and beyond; maps multiple frameworks	https://hitrustalliance.net/hitrust-csf
HIPAA Security/Privacy Rules → Any org handling U.S. healthcare data.	https://www.hhs.gov/hipaa
GLBA → Financial institutions managing consumer financial data.	https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act
SOX → Public companies, ensures integrity of financial reporting	https://www.sec.gov/news/press/2002-150.htm
GDPR → Anyone touching EU resident data.	https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en
PIPEDA / CPPA → Canadian organizations handling personal data.	https://priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda
CCPA / CPRA → U.S. orgs with California consumer data.	https://oag.ca.gov/privacy/ccpa
NYDFS Cybersecurity Reg. (23 NYCRR 500) → Financial services in New York	https://www.dfs.ny.gov/industry_guidance/cybersecurity
FFIEC CAT → Banks/credit unions assessing cyber resilience.	https://www.ffiec.gov/cyberassessmenttool.htm
NERC CIP → Energy/utilities; protects critical infrastructure.	https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx
FedRAMP → Cloud providers working with U.S. federal government.	https://www.fedramp.gov
ENISA Guidance → EU-focused, structured cybersecurity.	https://www.enisa.europa.eu/publications
OWASP ASVS / SAMM → Software/AppSec focused orgs.	https://owasp.org

Repost to help others

Wil Klusovsky | wilklu.me