CMMC合规必备：一份实用的网络安全 checklist

过去几年，我帮几个中小型制造商跑过CMMC（Cybersecurity Maturity Model Certification）的准备流程。每次开始，对方第一句话几乎都一样：“我们该从哪里下手？”不是没人知道要改，而是信息太散，标准文档厚得像一本小说。真正管用的，其实是一张能对着逐条打的 网络安全 checklist。

CMMC 2.0 把要求压到了三个级别，对多数分包商来说，Level 2 是现实目标。但纸上写“实施访问控制”和真正把域控制器配置对、把共享权限收拢，中间差着好几个通宵。下面这几条，是我在多家公司反复踩过坑之后，觉得最值得先钉死的项目。

资产清单：你不知道的，必没法保护

第一个常被跳过的基础动作，是拿出一份完整的资产清单。不是IT自己脑子里那串IP，而是每个连接到你网络的东西——打印机、摄像头、门禁控制器、甚至那个挂在会议室墙上的老旧iPad。我曾见过一家公司在审计前三天才发现，HR部门有一台没人记得的NAS，里面存着整年的员工W-2扫描件。CMMC的Level 2明确要求维护CUI（Controlled Unclassified Information）的流动记录，而资产清单一断，后面所有控制项都跟着断。

作法不复杂：用Nmap或类似工具扫一遍子网，然后人工核对每个设备的归属和用途。归类成“处理CUI”“接触CUI”“不接触CUI”三类，后面配置策略就好写得多。

多因素认证：别只在VPN上开

MFA在CMMC里几乎是硬门槛，但很多公司只把它开在远程VPN登录上。内部员工从办公室台式机访问财务系统呢？从车间Wi-Fi去查工单呢？我曾经审过一家供应商，VPN有MFA，但内部ERP用的是同一个本地AD账号加静态密码。审计员发现后直接开了观察项，整改周期压得团队很痛苦。

推MFA的关键不是技术，是说服用户。让工程师每天输六次验证码，他们会找办法绕过。我推荐的做法是：先挑一个应用（比如邮件或工时系统）做试点，选推送式验证而不是短信码，用户体验好，阻力就小。等大家习惯了，再铺到其他系统。

备份与恢复：测过才算真

备份策略几乎每家公司都说自己有，但“有备份”和“能恢复”是两回事。CMMC的RE（Recovery）控制点要求的不只是备份存在，还要求定期测试还原流程。我见过太多公司挂着每晚的备份日志，但从没试过从磁带里拉出一份文件。等到真的勒索病毒加密了文件服务器，才发现备份脚本半年前就静默失败了。

建议每季度做一次还原演练。不需要全量恢复，选一个关键共享文件夹，把最近的全备份和增量备份拉到隔离环境，确认数据完整、权限正确、应用能正常启动。把演练结果记下来，审计时能

直接拿出来当证据。

员工培训：别只放PPT

安全意识培训是CMMC Level 2的明确要求，但很多公司把它做成每年一次、员工坐在会议室看视频的仪式。效果？培训后一周我假扮IT支持发邮件“请点击重置密码”，上当率仍然超过40%。

真正能改变行为的培训，是小剂量、高频次、带情境的。每个月一次五分钟的模拟钓鱼测试，配合简短复盘——哪封邮件可疑、哪个链接不该点。不要惩罚上当的人，而是鼓励报告。我见过最好的做法是，在内部Slack频道里每周发一条“本周钓鱼线索”，像游戏一样让大家找。半年下来，点击率能降到个位数。

回到开头那张 网络安全 checklist，它不是一次性做完就扔的东西。CMMC认证真正的价值在于，它迫使你把安全从IT部门的项目，变成公司运营的一部分。每次做资产盘点、每回跑还原演练、每轮钓鱼测试，都在积累一种肌肉记忆。审计只是验证你已经养成的习惯。

修补管理：把漏洞窗口压到最短

补丁策略听起来平淡，但在现场我看到的违规案例里，大概有一半跟已知漏洞未修补直接相关。CMMC的MA（Maintenance）和SI（System Integrity）控制点都涉及及时修补，但“及时”在现实里是个拉扯。生产线上的控制器不能随便重启，ERP系统需要变更窗口，供应商的补丁发布节奏也不一致。

可行的办法是把资产按风险分级：直接处理CUI且面向互联网的系统划为Tier 1，补丁窗口压缩到72小时；内部办公系统划为Tier 2，一周内完成；专用设备或OT网络划为Tier 3，走变更评审流程但至少每月一次评估。分级之后，团队就知道什么该优先，什么可以缓一缓。

日志与监控：存够时长，但也要有人看

CMMC 2.0 要求保留审计日志至少一年。很多公司做到了存，却做不到查。日志堆在SIEM里，告警阈值设得要么太高（什么都漏），要么太低（每天几百条告警，没人读）。我见过一个团队因为告警疲劳，错过了AD域管理员账户凌晨三点的异常提权行为——直到业务部门说数据不对，才发现已经被横向移动过了。

更好的策略是缩小监控范围。不要试图记录一切，而是先定义“什么事件必须立即知道”：新增管理员账户、防火墙规则变更、大规模文件外拷、CUI目录的异常访问。把这几个场景写成简单规则，配合每周一次的日志抽样审查，比一个复杂但不被维护的系统有效得多。

写到最后，我想强调一件事。CMMC合规不是一场考试，你不需要一次做到完美。我合作过的公司里，做得最好的那些，都是从一张简单的 网络安全 checklist 开始，每个月只推进两三件事。半年后再回头看，差距已经小很多。关键是开始，然后持续。