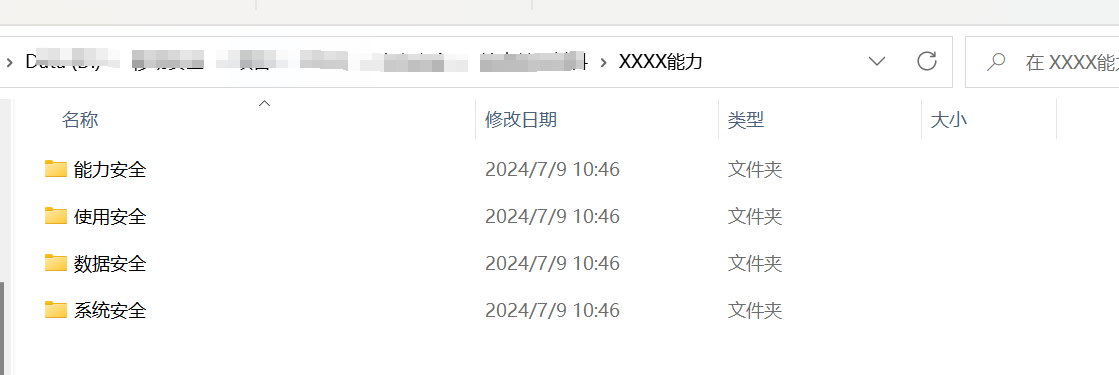
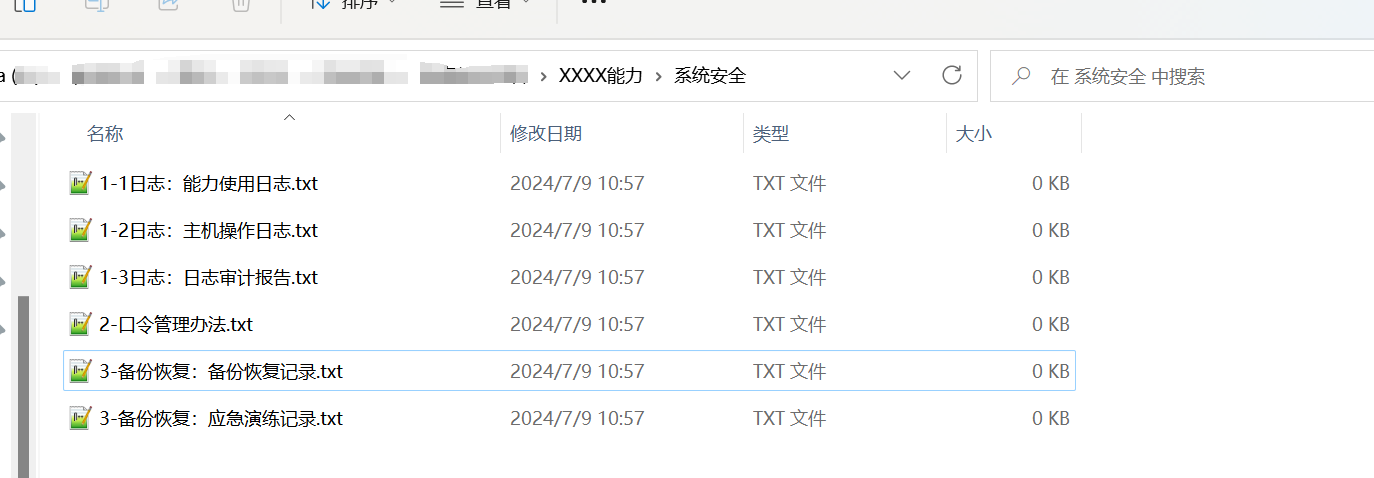
**中台检查文档需求清单**

**请各单位按照四个安全的角度对文档需求清单中的材料进行准备，推荐使用以下形式：**





**系统安全：**

1. 日志查验：
   1. 直接导出的能力迎检日起之前半年时间段的完整日志，包括能力使用日志、主机登录日志、主机操作日志、数据库操作日志、4A登陆日志等，不需要DEBUG级的日志，提供日志需要具备可读性；
   2. 迎检日起之前半年时间段的日志导出、查询、审计4A记录；
   3. 最新版本和次新版本的日志审计报告至少两份，与日志审计报告相关的通报、答复邮件。
2. 口令管理：
   1. 包含“口令管理”的原始设计文档，如口令管理办法；
   2. 弱口令扫描报告，扫描结果通报、答复邮件。
3. 备份恢复：
   1. 包含“备份恢复机制”“应急预案”的原始设计文档；
   2. 备份记录，如截屏、流程记录等；
   3. 最近一次应急演练记录。
4. 漏扫渗透：
   1. 最新版本和次新版本的漏洞扫描报告共计2份（9月份检查，提供8月和7月的）；
   2. 最新版本和次新版本的渗透测试报告共计2份（9月份检查，提供今年上半年做的1份，和今年下半年做的1份）。

**能力安全：**

1. 三同步：
   1. 包含“三同步”的制度文档；
   2. 项目在RMS、PMS中的关于系统安全建设的信息；
   3. 能力规划、能力建设和能力运行三个阶段，对能力进行安全管控、评审、批复的说明材料，定级备案。
2. 供应链安全：
   1. 软件物料清单；
   2. 外部软件安全评审材料；
3. 代码安全：
   1. 代码审计报告；
   2. 主机基线扫描报告。
4. 安全防护：
   1. 安全防护设备运行情况说明；
   2. 半年内安全防护设备维保记录。

**使用安全：**

1. 使用者管理：
   1. 外部使用协议或合同；
   2. 外部使用者统计信息；
   3. 外部使用者申请、订购记录。
2. 接口安全：
   1. 包含“接口访问控制”的设计文档；
   2. 接口安全测试报告；
   3. 接口访问控制策略。
3. 用户权限管理：
   1. 包含“用户权限说明”的设计文档；
   2. 导出用户与权限列表；
   3. 包含“异常行为监测”“特权账号监测”的设计文档；
   4. 账户监测记录；
   5. 账号审计报告。
4. 内容管控：
   1. 包含“不良信息管控”的设计文档；
   2. 不良信息管控机制。
5. 能力输出：
   1. 若将中台能力整合、二次包装推广销售，则提供新主体的安全管理要求（应包括保障网络安全、数据安全等方面）；
6. 能力使用（本单位在中台上订购的其他单位能力）：
   1. 订购能力清单；
   2. 订购能力数据安全管理材料，如输出、输出数据清单，涉敏数据管控材料；
   3. 订购能力账号安全管控材料，如账号列表、账号权限说明、账号登录日志、账号监控日志；
   4. 订购能力定期漏洞扫描报告。

**数据安全：**

1. 人员管理：
   1. 数据人员管理规范，包括不同人员的数据访问权限范围；
   2. 对三方人员访问数据的情况说明（包括账号统计、账号访问记录）；
2. 数据资产管理：
   1. 数据资产清单（能力涉及的数据输入、能力中间环节存储、能力处理完后的数据输出）；
   2. 数据分级分类保护说明文档；
3. 数据采集：
   1. 如进行数据采集，提供包含“数据采集告知”的协议；
4. 数据加密：
   1. 包含“数据脱敏、数据加密、去标识、模糊化等数据保护措施”的设计文档；
   2. 脱敏及数据模糊化处理证明材料；
   3. 金库访问申请审批记录、访问记录；
   4. 涉敏场景清单。
5. 数据销毁：
   1. 包含“数据删除”的设计文档；
   2. 数据删除效果证明材料；
6. 数据追溯：
   1. 证明数据处理可追溯性的材料。

**备注：**

1. 本清单以通用性的视角给出了自查时应当提供的材料范围，实际准备的材料应以具体的评估项需求为准；
2. 不同的中台能力、不同的主体提供的材料允许和本清单提供条目有所差异，但提供的材料应包含该能力涉及的所有评估项所需内容；