**WHAT’S ALREADY DONE**

**1. PROJECT STRUCTURE & DELIVERABLE CHECKLIST**

| **Folder** | **Deliverable** | **Description** | **Status / Notes** |
| --- | --- | --- | --- |
| **01\_charter** | Project\_Charter\_v1.pdf | Overview of company, objectives, roles, key metrics (KPIs), and governance. | ✅ Draft done (needs small update and improvement) |
| **02\_assets\_flows** | Stakeholders\_Assets\_v0.xlsx | Inventory of all assets (people, systems, data, applications) with owners and criticality. | ✅ Done — needs improvement and update (remove YAML mention, merge customer/product DB, include CRM – what else? |
| **03\_architecture** | Architecture\_v0.drawio | Diagram showing SaaS, VPN, network segmentation, and connections between HQ, branch, and remote users. | ✅ Completed by Nerses (make sure SaaS apps appear **outside** corporate perimeter). Final comments from lecturer will be received on Friday |
| **04\_controls\_policies** | Controls\_Shortlist\_v0.docx | List of chosen CIS v8 and NIST CSF controls (mapped to ID/PR/DE/RS/RC). | ✅ Done — can be expanded with 1–2 extra controls (e.g., backup immutability, password policy). |
| **05\_implementation** | (Playbooks, Runbooks, Scripts, etc.) | Includes SOC playbook, incident response procedure, seeder script or Excel-based inventory. | ✅ Done — Playbook file. |
| **06\_validation** | (Reports, metrics, testing results) | Evidence of control validation — e.g., MFA enabled, EDR deployed, SIEM tested, etc. | ❌ Not yet — can create simulated validation report or KPI metrics summary. |
| **07\_presentation** | Final presentation (slides) | Team summary of project for teacher review — 5–7 slides. | ❌ To do last. |

**2. COMPANY PROFILE (must appear in Charter)**

| **Element** | **Description** |
| --- | --- |
| **Company Name** | EasyBusy |
| **Type** | Mid-sized e-commerce company |
| **Staff** | 50 employees — HQ (40) + branch (10); 20% remote (10 total) |
| **Departments** | Sales & Marketing, Customer Support, IT, Finance, Operations, Management |
| **Key Assets** | Cloud email & files (Microsoft 365), Accounting SaaS, CRM, E-commerce platform, Customer DB |
| **Key Risks** | Phishing, credential theft, data leakage, ransomware |
| **Budget** | CapEx ≤ $20k; OpEx ≤ $1.5k/month |
| **Main Goal** | Implement foundational cybersecurity controls aligned with NIST CSF (ID/PR/DE/RS/RC) |

**3. NIST CSF + CIS v8 MAPPING (we have this in charter, maybe should be improved)**

| **NIST Function** | **CIS v8 IG1 Controls (examples)** | **Project Action** |
| --- | --- | --- |
| **Identify (ID)** | 1.1–1.6: Asset inventory, ownership | Excel-based asset register |
| **Protect (PR)** | 4.1–6.6: MFA, backups, privilege management | MFA 100%, least-privilege model |
| **Detect (DE)** | 8.2–8.7: Logging, SIEM alerts | SIEM/MDR integration, triage |
| **Respond (RS)** | 17.1–17.5: Incident response plan | IR playbook + runbooks |
| **Recover (RC)** | 11.2–11.4: Recovery planning | Backup immutability, RPO/RTO policy |

**4. Security Operations Lead (Karine) – I submitted this:**

✅ Completed:

* SOC monitoring strategy (EDR + SIEM + alerts)
* Incident Response Playbook
* KPI tracking list
* Rules for employees
* Weekly operational checklist
* **SOC Governance (RACI matrix)** — who’s responsible/accountable/consulted/informed.
* **Runbooks (3–4)** — practical step-by-step for common incidents (e.g., phishing, ransomware, lost laptop).
* **Post-Incident Report Template** — short, standard form.
* **Quarterly SOC Review Plan** — metrics, lessons learned, improvement cycle.

**5. MISSING OR IMPROVEMENT AREAS**

| **Area** | **Missing** | **Solution** |
| --- | --- | --- |
| **Validation Evidence** | Absent | Add report with screenshots or fake data showing controls tested |
| **KPI Dashboard** | Only listed | Simulate a chart or table of progress per control |
| **Presentation** | Missing | Create PowerPoint (we can do this together later) |

**✅ SUMMARY OF WHAT YOU HAVE NOW (as of today)**

| **Category** | **Status** |
| --- | --- |
| Charter | ✅ (needs update with full company description and new rules) |
| Asset Inventory | ✅ (Excel version preferred) |
| Architecture Diagram | ✅ Done |
| Controls Shortlist | ✅ Done (can be expanded slightly) |
| Playbook | ✅ (IR procedure completed) |
| Runbooks | ✅ Done (can be expanded slightly) |
| SOC Governance / RACI | ✅ Done |
| KPI Tracking | ✅ Done |
| Validation Report | ❌ (to be simulated) |
| Presentation | ❌ (to be done at the end) |