The Cybersecurity lifecycle differs between greenfield and brownfield projects

1. Identify *(NIST: Asset Management, Risk Assessment; ISO 27001: Context of the Organization, Risk Assessment)*

Greenfield	**Brownfield**
- Define **security requirements** before system design. - Build asset inventory from day one with full visibility. - Threat modelling before deployment.	- Conduct **security posture assessment** of existing environment. - Identify gaps in existing inventory (shadow IT, unmanaged assets). - Reverse-engineer threat modelling based on known vulnerabilities and legacy systems.

2. Protect *(NIST: Access Control, Data Security, Protective Technology; ISO 27001: Controls Implementation)*

Greenfield	**Brownfield**
- Implement **security-by-design** controls: Zero Trust, MFA, encryption at rest/in transit. - Role-based access control from day one. - Harden configurations before go-live.	- Layer security controls onto existing architecture. - Reconfigure access control lists, deploy encryption where missing. - May require temporary compensating controls until legacy upgrades happen.

3. Detect *(NIST: Anomalies & Events, Continuous Monitoring; ISO 27001: Monitoring & Measurement)*

Greenfield	**Brownfield**
- Integrate **SIEM/SOC monitoring** and logging during system build. - Establish baselines from the start. - Design for visibility (network taps, logging APIs).	- Implement monitoring tools over existing environment (often piecemeal). - Build baselines from mixed/legacy data. - May need network segmentation first to enable better detection.

4. Respond *(NIST: Response Planning, Communications; ISO 27001: Incident Response Plan)*

Greenfield	Brownfield
- Incident response playbooks written alongside system deployment. - Tabletop exercises before production cutover. - Digital forensics capability embedded in architecture.	- Retrofit incident response to cover legacy systems. - Address missing logging sources to support forensics. - May have to adapt playbooks to account for older tech that can't support rapid containment.

5. Recover *(NIST: Recovery Planning, Improvements; ISO 27001: Continual Improvement)*

Greenfield	Brownfield
- Build **resilience** from the start (redundancy, backups, DR sites). - Recovery plans tested before go-live. - Use modern orchestration for rapid restore.	- Assess existing DR capabilities, often upgrade incrementally. - Address backup gaps (incomplete, unencrypted, or untested backups). - Recovery processes may require staged modernization.

Summary Table (Lifecycle View)

NIST CSF Function	Greenfield	Brownfield
Identify	***Start fresh with full asset & threat mapping***	***Reverse-engineer visibility into existing systems***
Protect	***Embed modern controls from day one***	***Retrofit controls with minimal disruption***
Detect	***Build monitoring into design***	***Bolt-on monitoring to legacy systems***
Respond	***Plan and test before launch***	***Adapt to existing system constraints***
Recover	***Resilience by design***	***Gradual DR improvements***