

Service Effectiveness and Maturity

Chris Andes



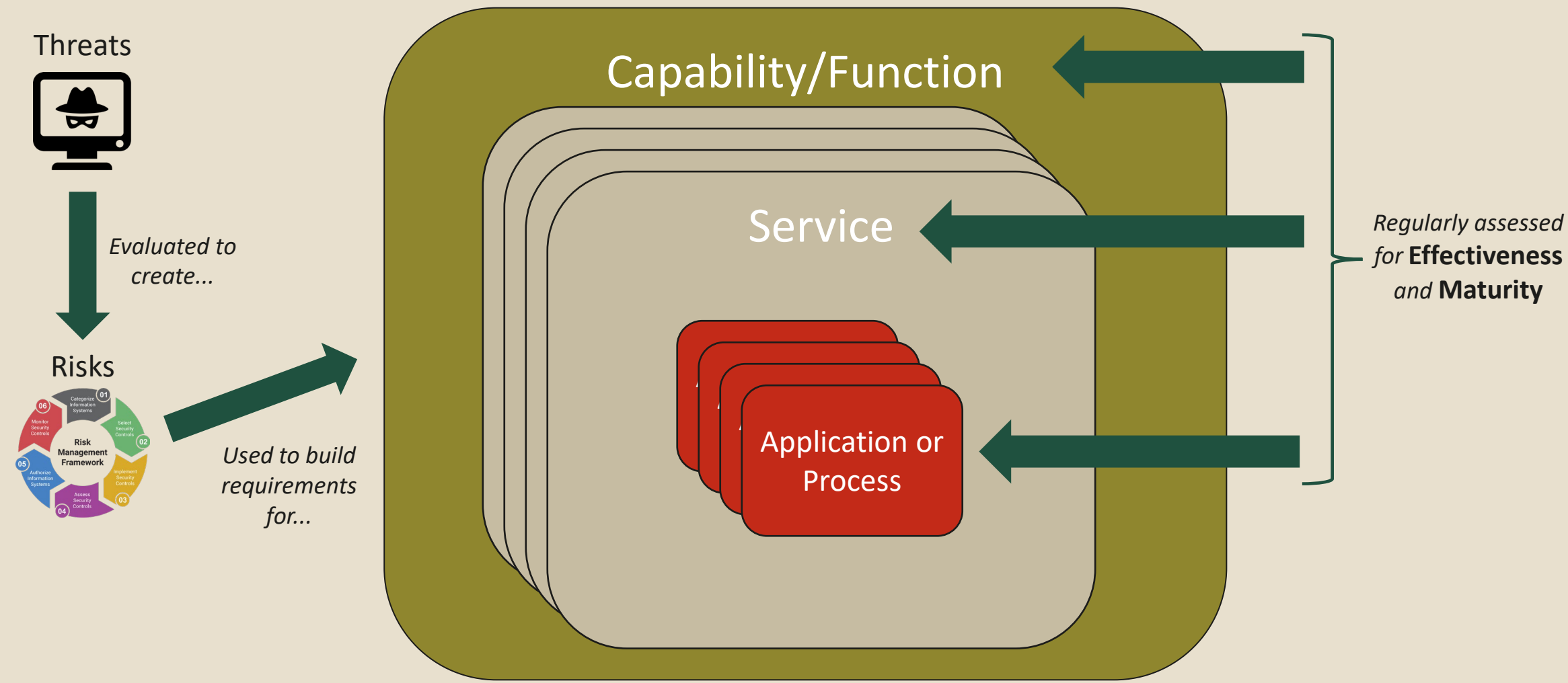
Topics

- ☐ Defining Security Functions
- ☐ Assessing Maturity
- ☐ Assessing Effectiveness
- ☐ Calculating Service E&M
- ☐ Examples

WHY?

- ❑ Programmatic approach to assessing InfoSec and Privacy Functions
 - ✓ Creates a standard for how we look at our services
 - ✓ Gap areas are visible to the entire department
 - ✓ Provides a systematic method to road mapping
 - ✓ Resource prioritization
 - ✓ Deconfliction of function responsibilities
- ❑ Introduction to the methodology that will be using to assess services.

Definitions



Assess the Service Maturity

Scoring capabilities and security practices is an important part of understanding where an organization currently stands and where investment is needed.

- Use the Capability Maturity Model Integration (CMMI).
- Service maturity is a **qualitative** assessment measuring the **processes** and **management** around a service



Level 5 (Optimized)
Focus on continuous process improvements

Level 4 (Managed)
Process measured and controlled

Level 3 (Defined)
Process characterized for the organization and is proactive

Level 2 (Managed)
Process unpredictable, poorly controlled and reactive

Level 1 (Initial)
Process unpredictable, poorly controlled and reactive

Level 0 (Does Not Exist)
Ad-hoc

Assessing the Service Maturity

Maturity Levels	Roles and Responsibilities	Policy/Procedure Management	Audit and Monitoring	Reporting
Level 0 (Does Not Exist) Ad-hoc	-	-	-	-
Level 1 (Initial) Process unpredictable, poorly controlled and reactive	No InfoSec/Privacy representative assigned or support structure in place for the business. Information InfoSec/Privacy issues are not identified mitigated by qualified resources using the defined processes.	Minimal or no InfoSec/Privacy policies, procedures, or guidelines exist. Documentation is not stored in a central location.	Business does not conduct any self-assessments; No controls in place to ensure information (e.g., PII, intellectual property) is protected according to information security policy.	Business does not collect or report on information security metrics.
Level 2 (Managed) Process unpredictable, poorly controlled and reactive	No InfoSec/Privacy representative assigned within the business. Alternative support structure may exist. Information InfoSec/Privacy issues are identified on a ad-hoc fashion. Issues may me escalated to be mitigated. Limited consistency in the process.	InfoSec/Privacy policies, procedures, and guidelines for major of areas are documented and available in a central location. Policies are approved by policy owners and key stakeholders. Policies delineate information InfoSec/Privacy management structure, clearly assign information InfoSec/Privacy responsibilities, and lay the foundation necessary to reliably measure progress and compliance. Policies identify specific penalties and disciplinary actions to be used if the policy is not followed.	Self-assessment criteria are documented and is known. Business does conduct random self-assessments, but is not a formalized process to include and/or perform within existing business activities.	Metrics are identified and scorecard is created.
Level 3 (Defined) Process characterized for the organization and is proactive	InfoSec/Privacy lead/SME assigned; R&R for the lead is understood.	InfoSec/Privacy policies, procedures, and guidelines for all areas are documented. Clearly define information InfoSec/Privacy responsibilities and expected behaviors for asset owners and users, information resources management and data processing personnel, management, and IT InfoSec/Privacy administrators. New employees are briefed on company and business unit InfoSec/Privacy policies.	Self-assessment criteria are documented, and monitoring tools are available to automate the process. Self-assessments are performed regularly and is integrated into existing business activities.	Metrics are approved by management and procedural documentation is created and documented.
Level 4 (Managed) Process measured and controlled	InfoSec/Privacy lead/SME assigned; Established integration with the InfoSec/Privacy community. Representative is a InfoSec/Privacy advocate and an influencer. Roles and responsibilities are defined and followed.	Procedures are communicated to individuals who are required to follow them. Information security procedures and controls are implemented in a consistent manner everywhere that the procedure applies and are Organizationnforced through training. Initial testing is performed to ensure controls are operating as intended.	Self-assessment criteria is regularly evaluated and updated to mitigate against newly identified risks. Self-assessment and/or monitoring results are correlated and used to identify mitigating controls and metrics.	Metrics are being tracked and reported to management.
Level 5 (Optimized) Focus on continuous process improvements	InfoSec/Privacy role hierarchy exists; Responsibilities are defined based on the InfoSec/Privacy needs and advancements; Roles are defined to provide the highest level of support.	Effective implementation of information security controls is second nature. Policies, procedures, implementations, and tests are continually reviewed and improvements are made. Information security is an integrated practice. Threats are continually reevaluated, and controls adapted to changing IT security environment.	Self-assessment/monitoring program is fully operational. Status metrics for self-assessment program are established and met. Comprehensive self-assessment/monitoring program is an integral part of the culture.	Metrics are fully operational and reported to management. Trends are identified and areas that need to be addressed are prioritized.

Assessing Service Effectiveness

Service effectiveness is a ***qualitative*** measurement of the **value** this service brings to the organization. Effectiveness should answer the question “how well does this service address the risk”.

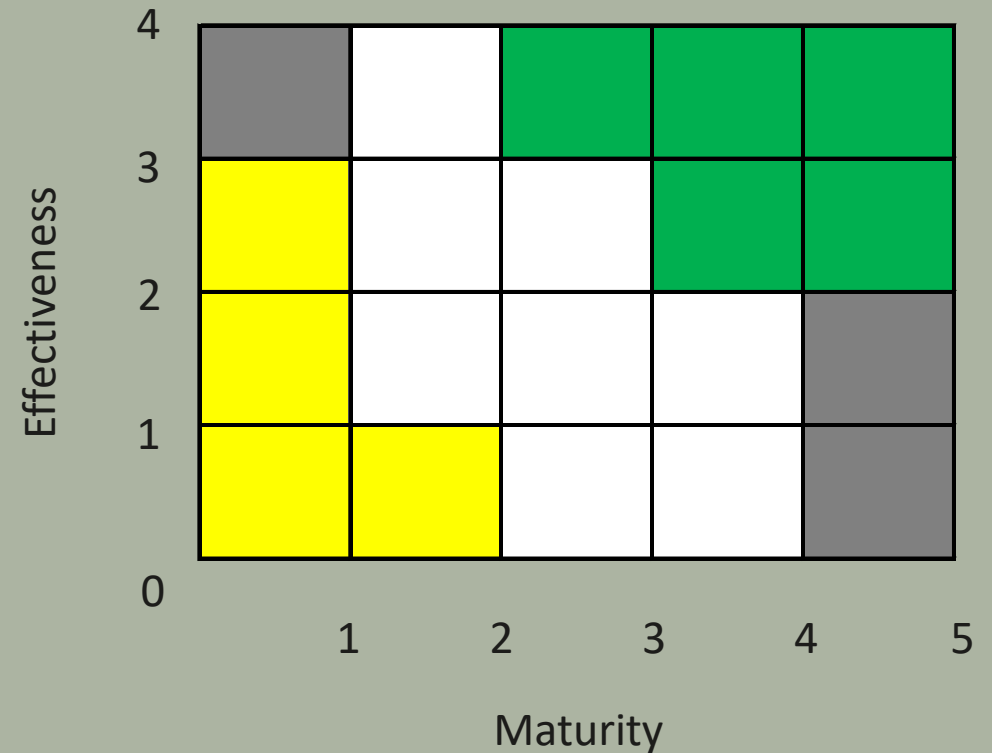
	Technical Fit	Scope	Business Fit (Functionality)
Level 0 Service or application does not exist	-	-	-
Level 1 Inappropriate or insufficient	Replacement mandatory to satisfy the service requirements	Deployment/use scope not adequate (testing or POC)	Not enough or wrong functionality
Level 2 Minimally effective	Replacement recommended to satisfy the service requirements	Deployed to a small subset of uses/assets to meet some service requirements	Rudimentary functional support
Level 3 Adequate or sufficient	Some parts could be optimized	Adequately deployed to meet minimum service goal	All major functions exist
Level 4 Fully appropriate and fully available	No change needed apart from regular maintenance	Fully deployed, used, and/or implemented	High number of functions available

Service Assessment

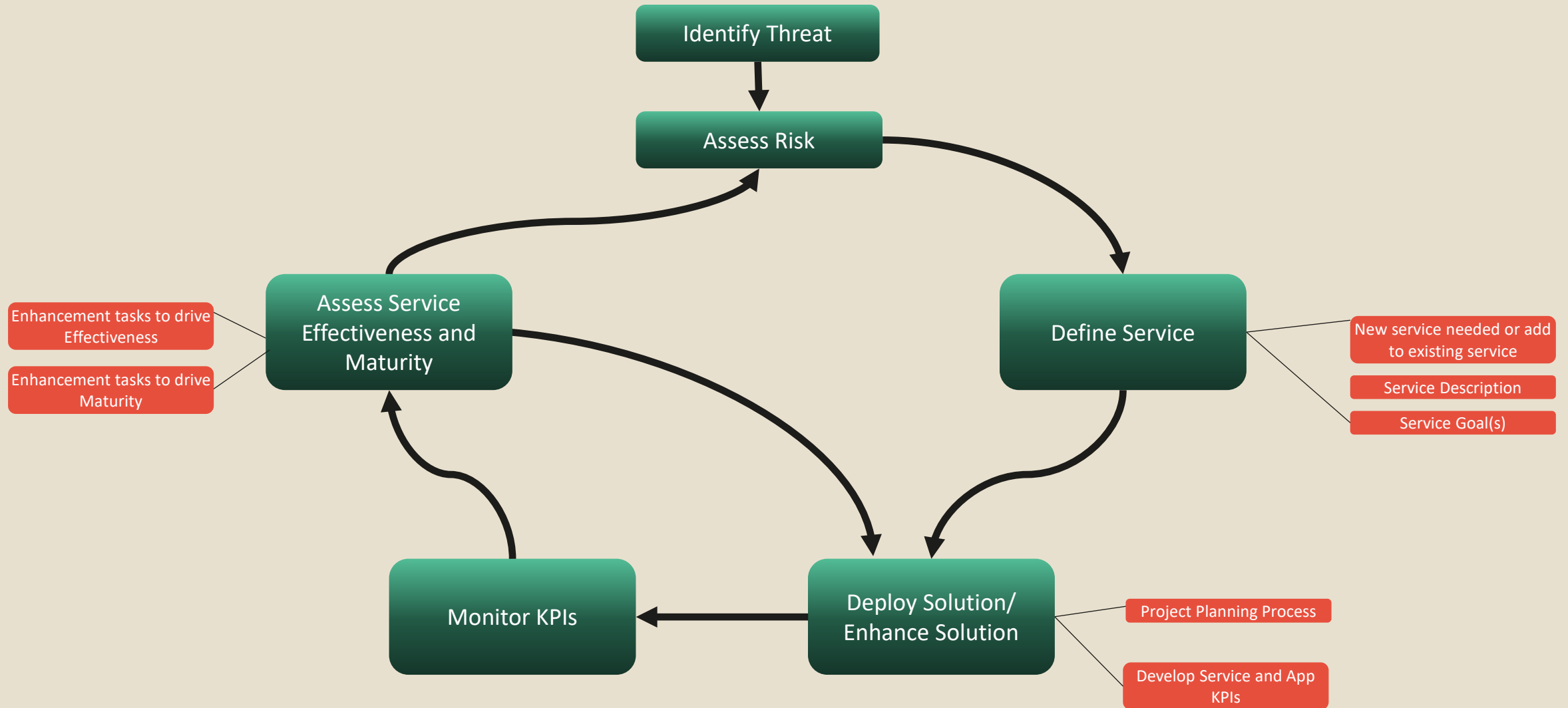
Value & Process


Service assessment is a **quantitative** measurement based on the **qualitative** scoring for the service in its Effectiveness and Maturity. The value computed will indicate the overall service assessment and can be categorized into 3 phases:

- **Envisioning**
- **Developing**
- **Optimizing**



Putting it all together and Example



A stylized line drawing of a desert landscape in the bottom left corner. It features rolling hills, two saguaro cacti, and a large circle representing the sun or moon. Three wavy lines above the hills represent birds in flight. The background is split into a light cream color on the left and a textured sage green on the right.

NEXT STEPS

- ☐ Service Inventory
- ☐ Service Descriptions

Appendix

Definitions

1. **Application** — A software organization of related functions, or series of interdependent or closely related programs, that when executed accomplish a specified objective or set of user requirements
2. **Capability** — A capability describes what an organization needs to be able to do in order to execute its strategies, realize specific outcomes and goals, and create value for its customers and other stakeholders.
3. **Effectiveness** — The capability of producing a desired result or the ability to produce desired output.
4. **Function** — Primary unit within the Cybersecurity Framework. Exhibits basic cybersecurity activities at their highest level.
5. **Maturity** — The ability of an organization for continuous improvement in a particular discipline
6. **Risk** — A measure of the extent to which Organization is threatened by a potential circumstance or event, and typically a function of the adverse impacts that would arise if the circumstance or event occurs and the likelihood of occurrence.
7. **Service** — Providing something of value to a customer that is not goods (physical things with material value). Or; A mechanism to enable access to one or more capabilities
8. **Threat** — Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service, or something or someone that can intentionally or accidentally exploit a vulnerability.

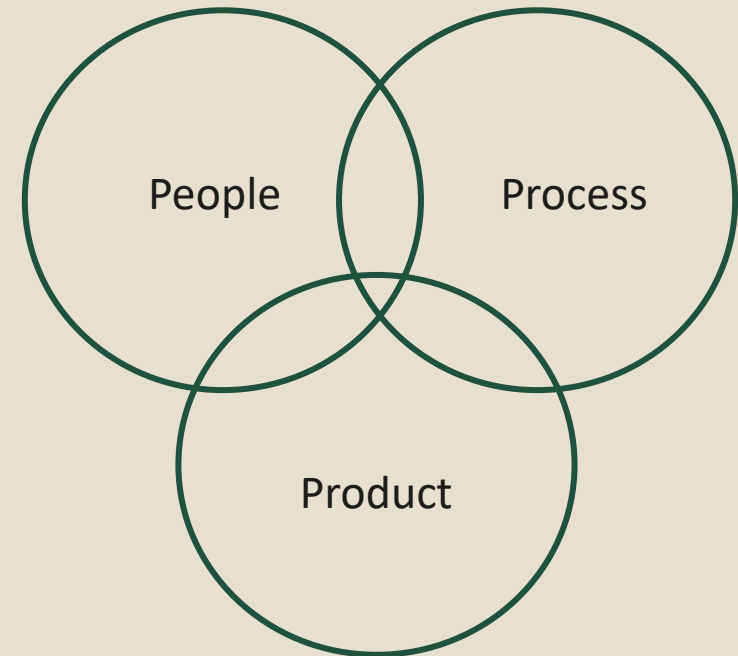
Define the Service

Defining the service answers the question “how will you solve for the threat/risk”. The first step is to see if the new threat can be added to a current service, if not a new service definition should be created.

Steps:

- Define overall goal of service
- Determine appropriate solutions (3Ps)
- Deploy solutions
- Create service/application KPIs
- Assess (and reassess) effectiveness and maturity

*Options to Support Service Requirements
(3Ps)*



Security Functions

Security functions defined in NIST Cyber Security Framework:

- **IDENTIFY:** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities
- **PROTECT:** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **DETECT:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **RESPOND:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **RECOVER:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.



IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Identity Management, Authentication and Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Management Strategy	Information Protection Processes and Procedures		Mitigation	
	Maintenance		Improvements	
	Protective Technology			

Solving for Threats/Risk

Identifying threats is the most important step to building a security service and deploying appropriate applications. Risk is derived from threats; and services are created to reduce risk. So, without an understanding of the threat, there is no way to accurately build or enhance a service.

Try not to build a threat statement that calls out a specific application for remediation.

Writing a threat statement:

- Use basic interrogatives (5Ws) – *who, what, where, when, why*
- Prioritize **What** and **Why**
- Good Ex: *Threat actors exploit vulnerable service on infrastructure devices to gain access to sensitive data, gain network foothold, or conduct other unauthorized activity.*
- Good Ex: *EU Auditors leverage fines on Organization based on non-compliance to ePrivacy Directive in relation to site tracking cookies.*
- Bad Ex: *Deploy CrowdStike to reduce the risk to client system*