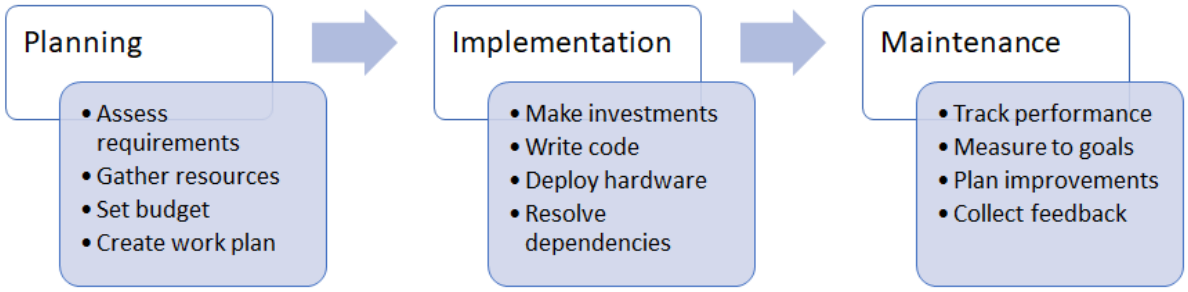
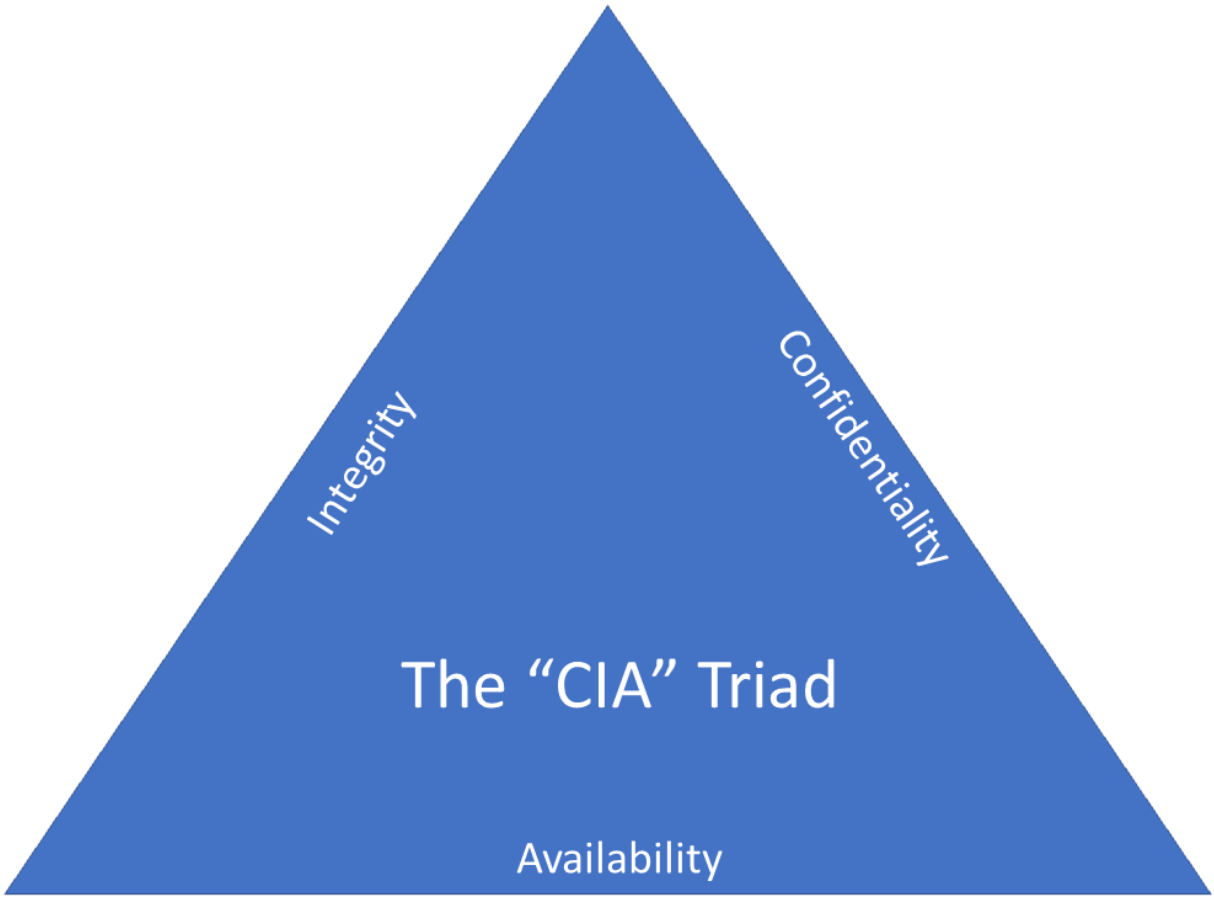
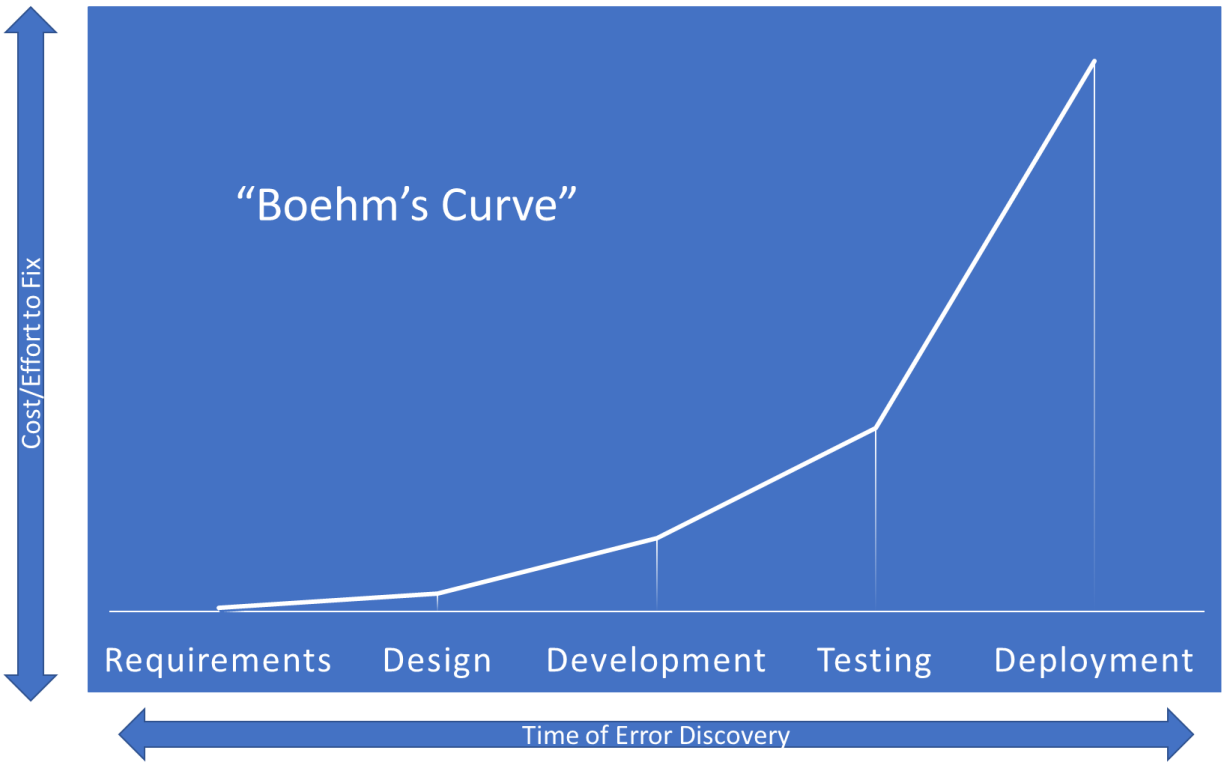
Chapter 1: What is Cybersecurity Architecture?



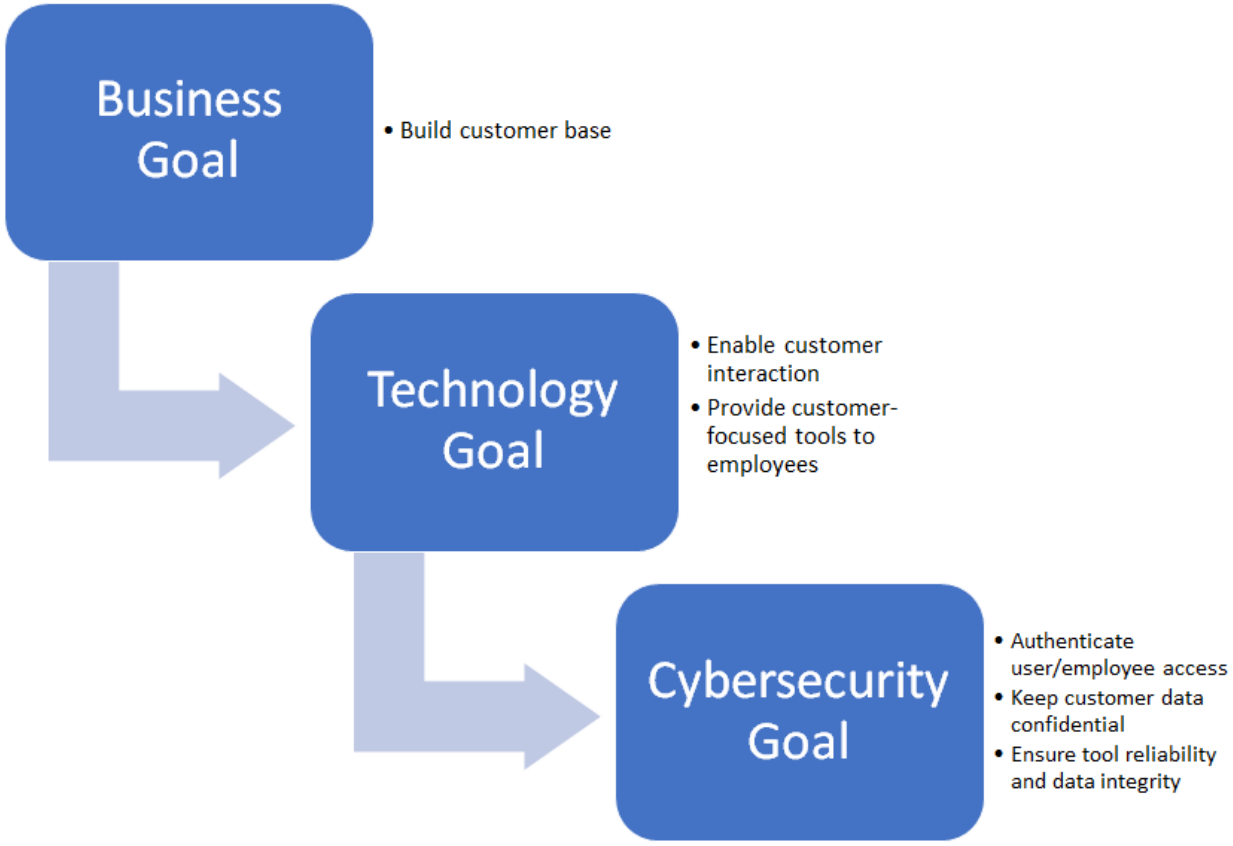


Application	• Directly services end users • Examples: HTTP, FTP
Presentation	• Transforms data (e.g. encryption, compression) for applications • Examples: TLS, media encoding
Session	• Governs “connections”: session establishment, maintenance • Examples: NetBIOS, RMI, RPC
Transport	• Provides “host to host” communication, error control, segmentation • Examples: TCP, UDP
Network	• Routes data (packets) between networks via addressing • Examples: IP, ICMP
Data Link	• Link between network elements (nodes) • Examples: Ethernet, WiFi (802.11)
Physical	• Physical transmission medium • Examples: RJ45, RJ11, coaxial cabling

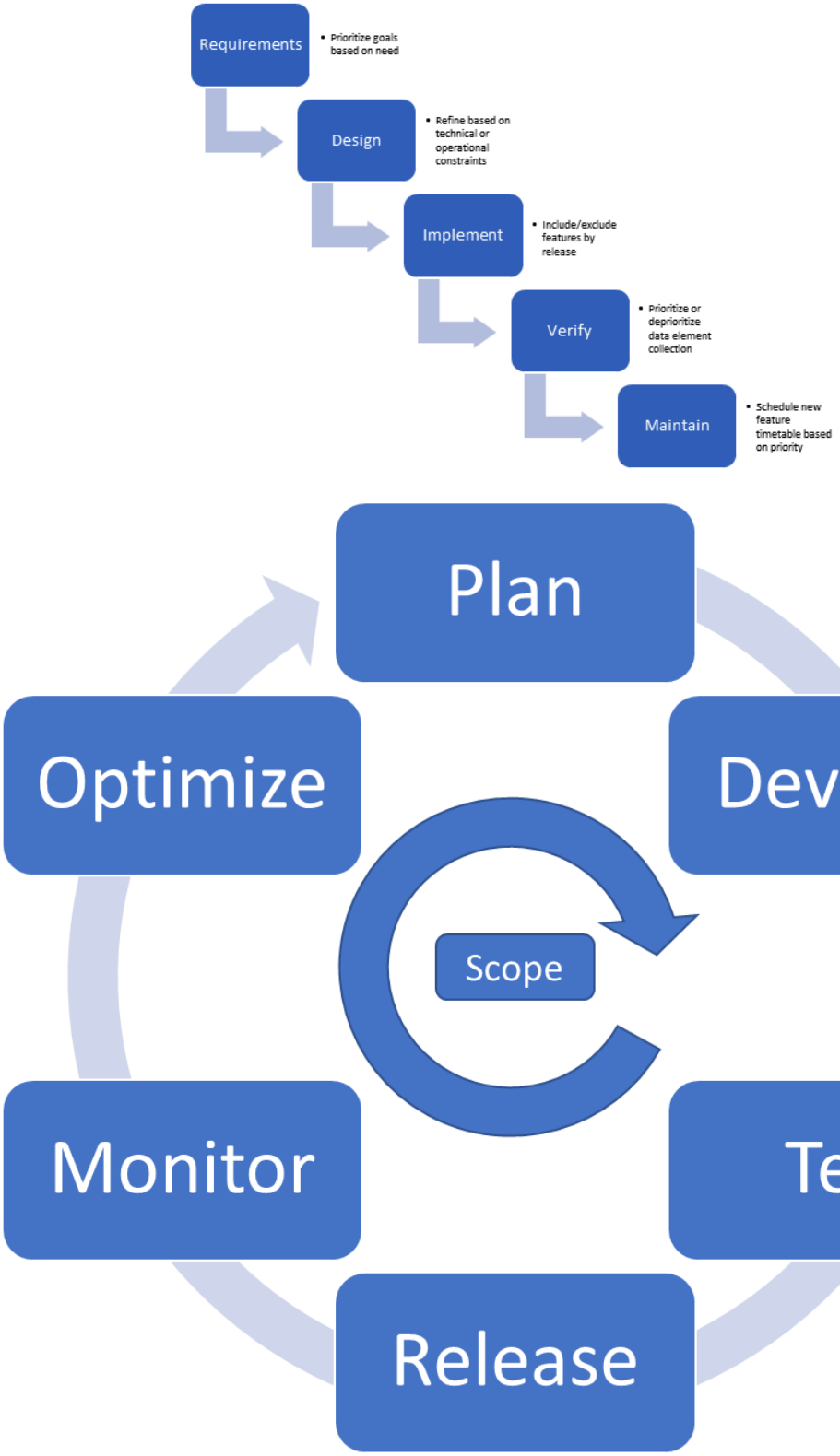
Application	• Directly services end users • Examples: HTTP, FTP
Transport	• End-to-end communication, error-controlled delivery • Examples: TCP, UDP
Internet	• Routing, host addressing, traffic control • Examples: IP, ICMP
Link (network interface)	• Physical media/transmission, hardware addresses, frame synchronization • Examples: Ethernet, ARP, 801.11

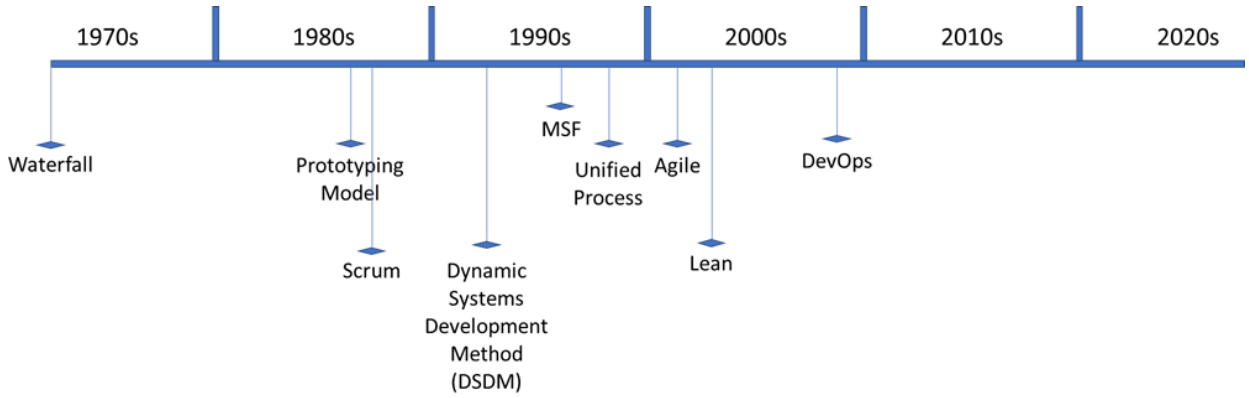

"Boehm's Curve"
Cost/Effort to Fix
Requirements
Design
Development
Testing
Deployment
Time of Error Discovery

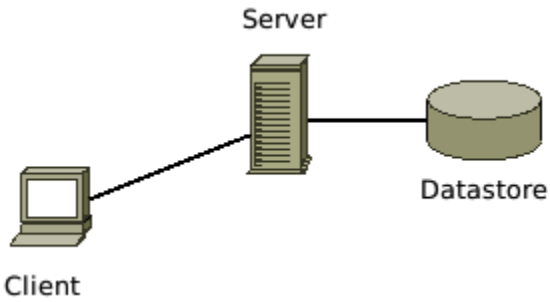
Chapter 2: The Core of Solution Building

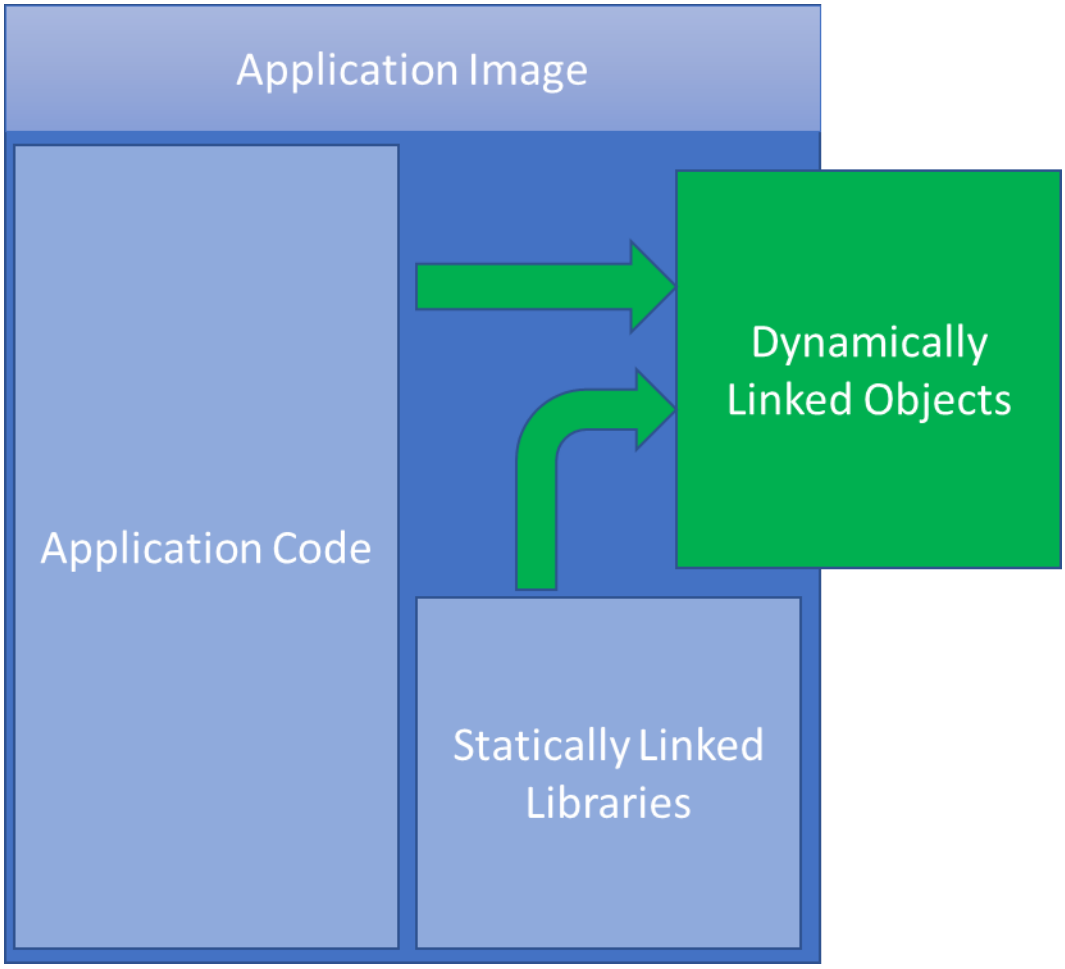


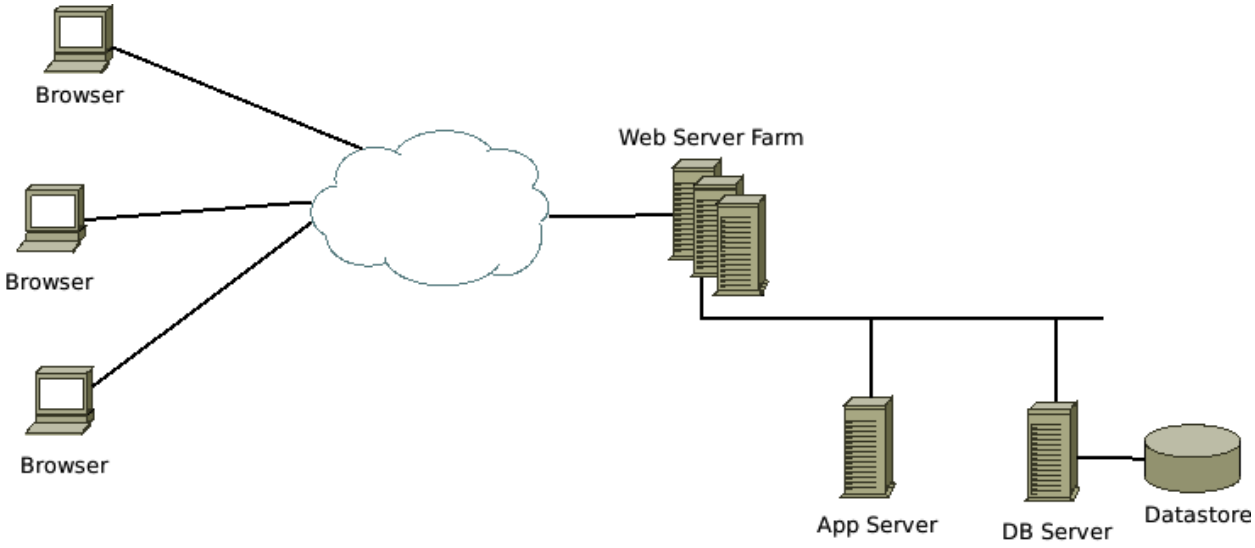
Chapter 3: Building an Architecture – Scope and Requirements

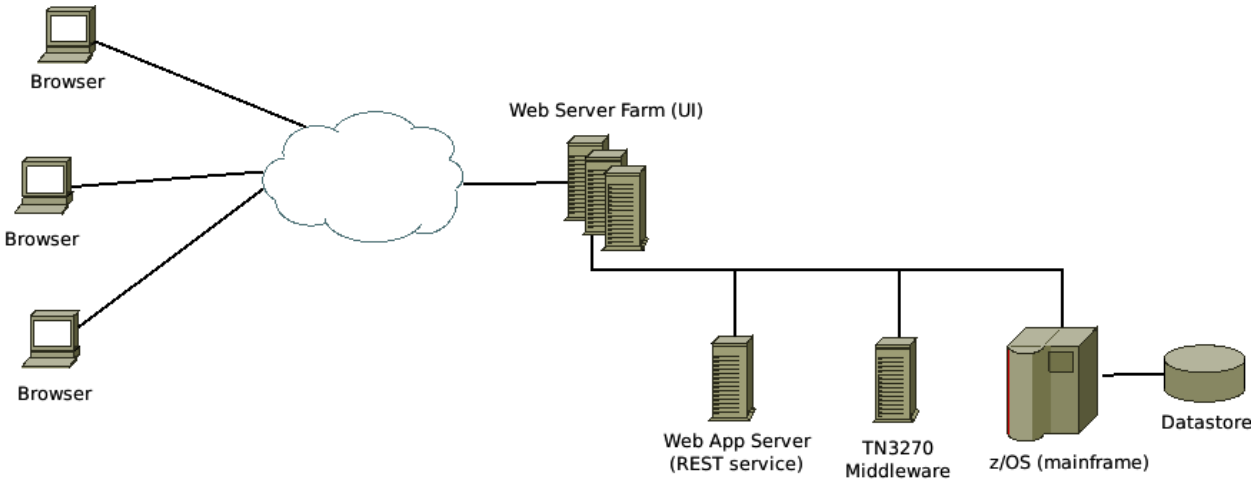



1970s
1980s
1990s
2000s
2010s
2020s
Waterfall
Prototyping Model
Scrum
Dynamic Systems Development Method (DSDM)
MSF
Unified Process
Agile
Lean
DevOps

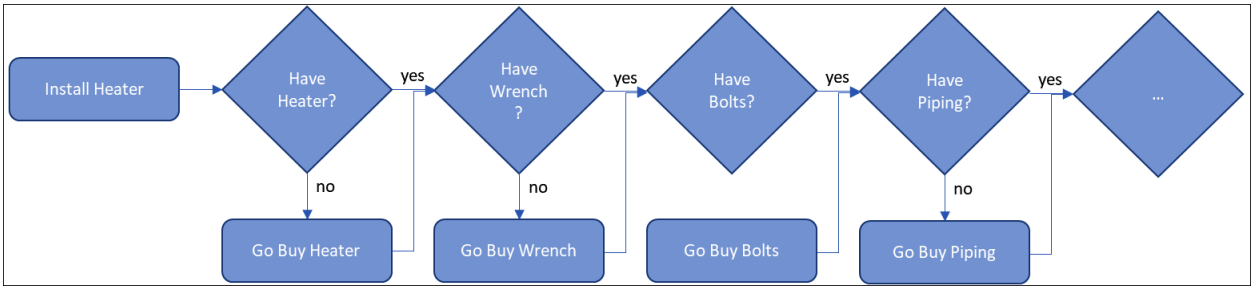

Server
Datastore
Client

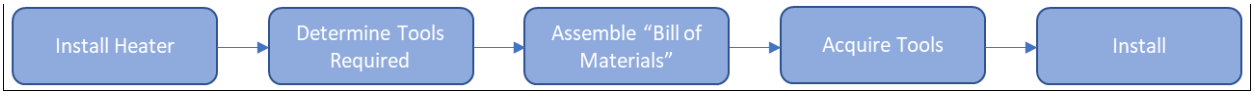

Application Image
Application Code
Dynamically Linked Objects
Statically Linked Libraries

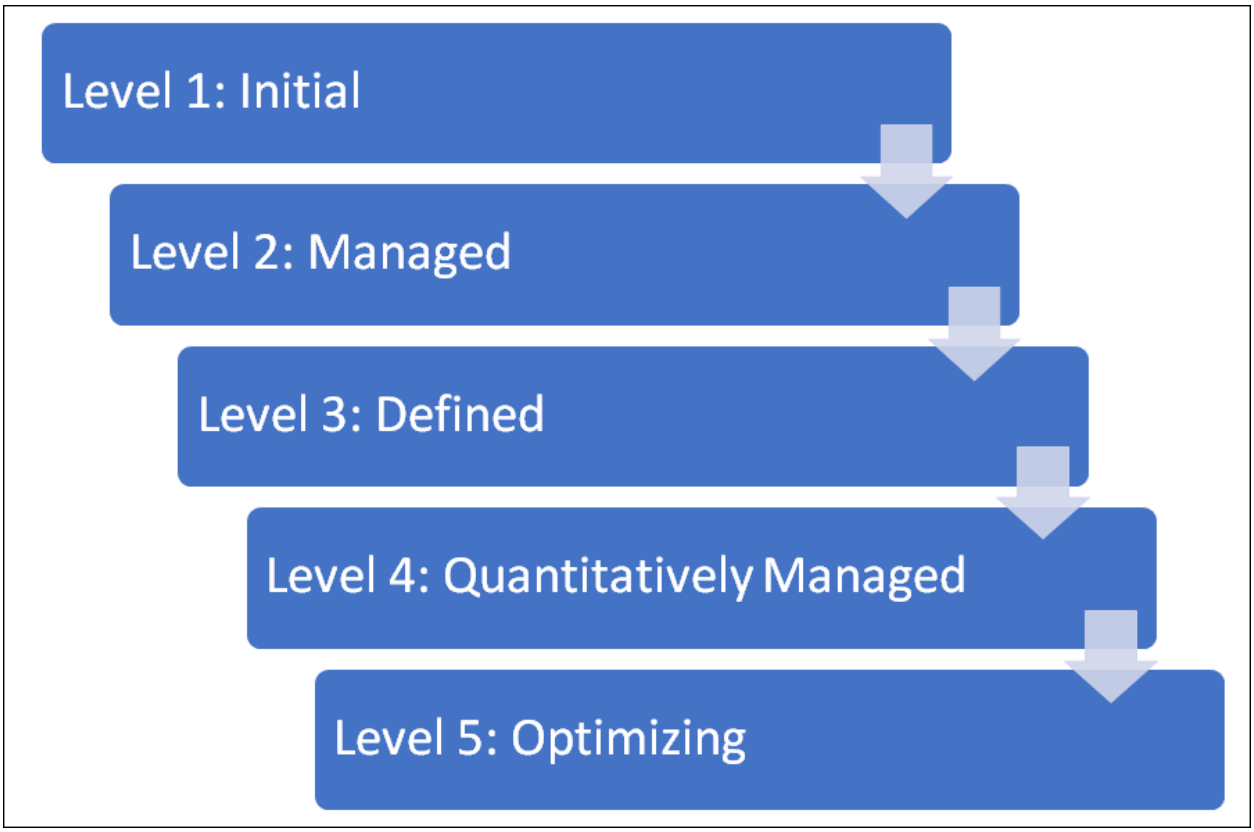

Browser
Browser
Browser
Web Server Farm
App Server
DB Server
Datastore


Browser
Browser
Browser
Web Server Farm (UI)
Web App Server
(REST service)
TN3270
Middleware
z/OS (mainframe)
Datastore

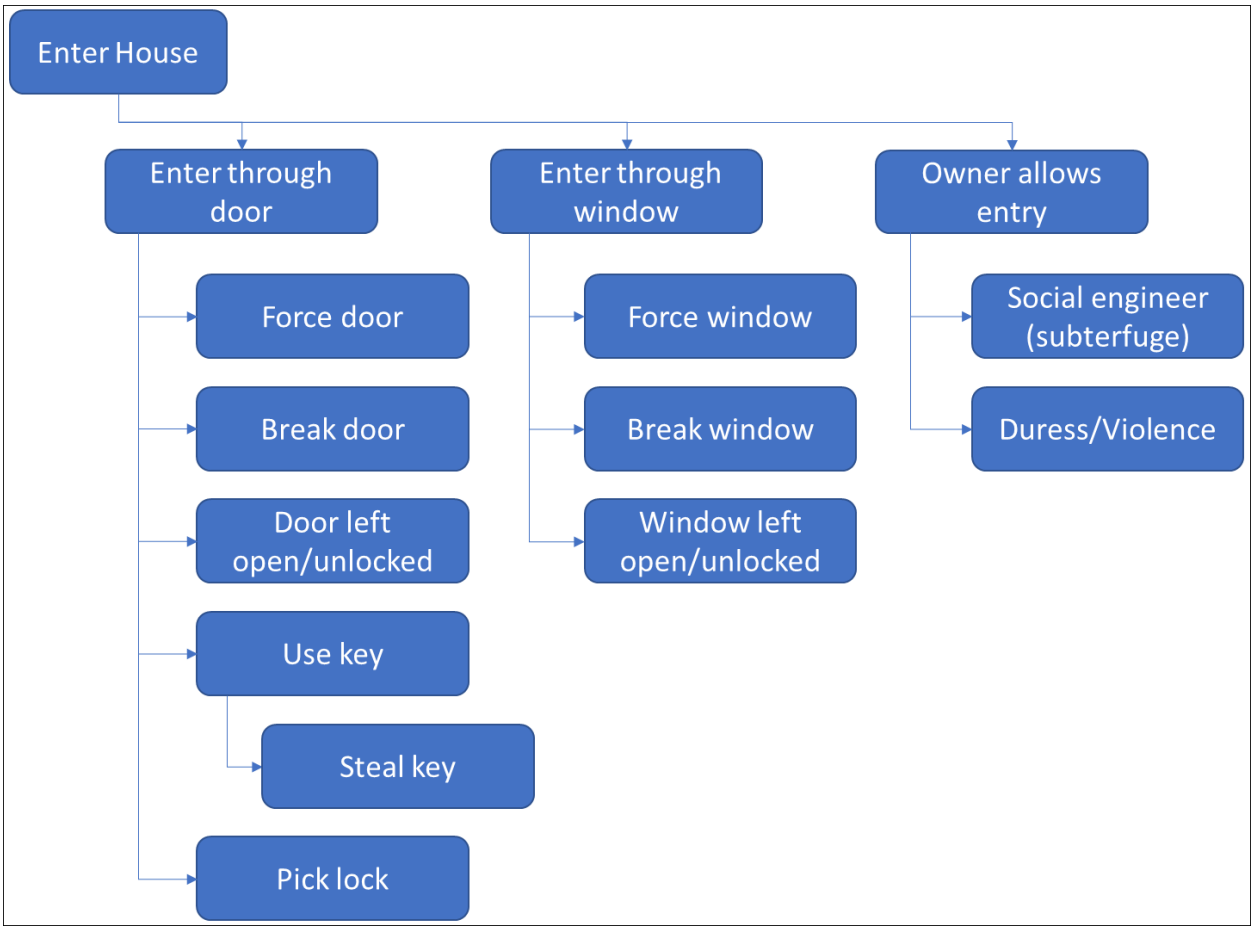
Chapter 4: Building an Architecture – Your Toolbox

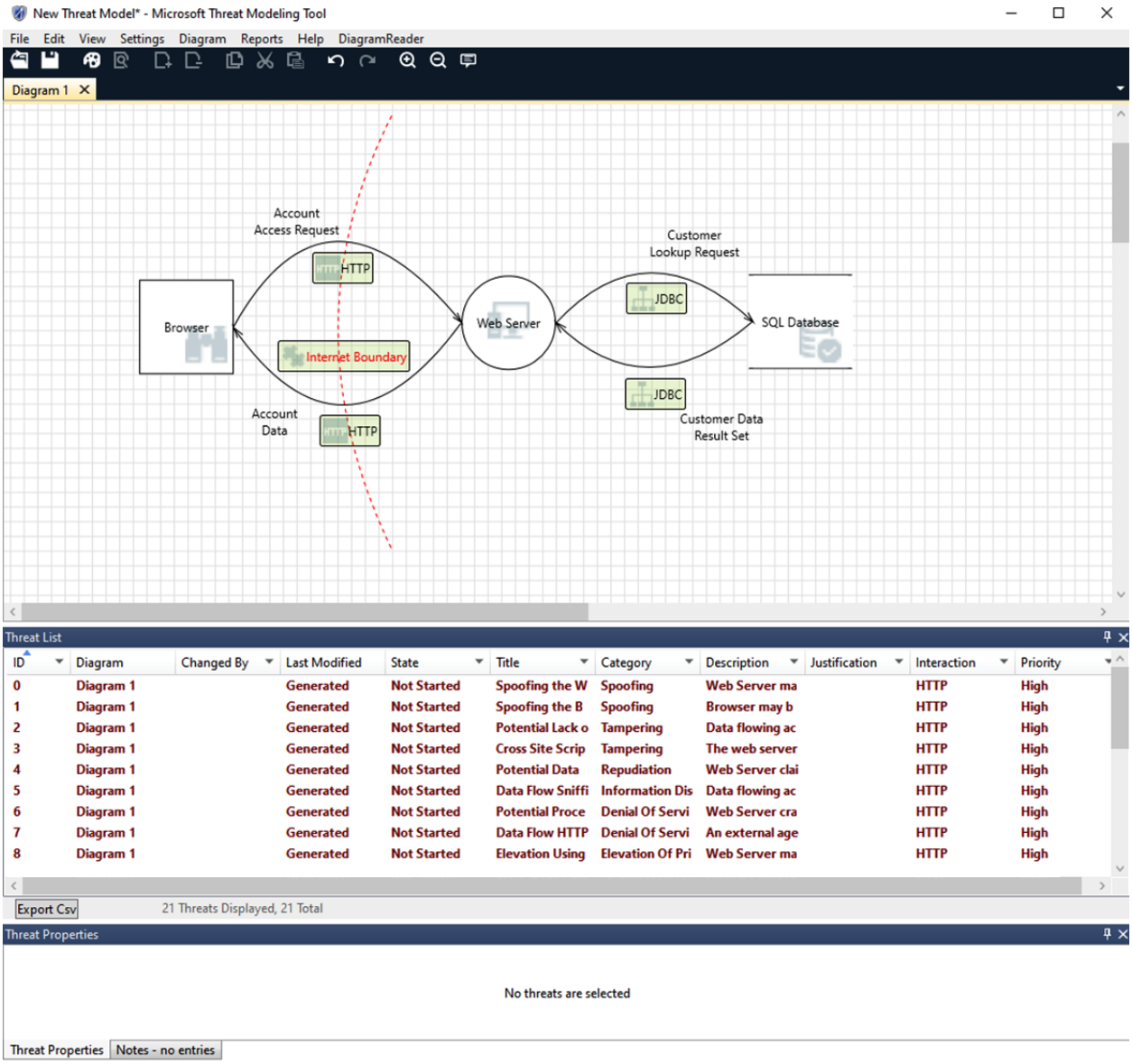




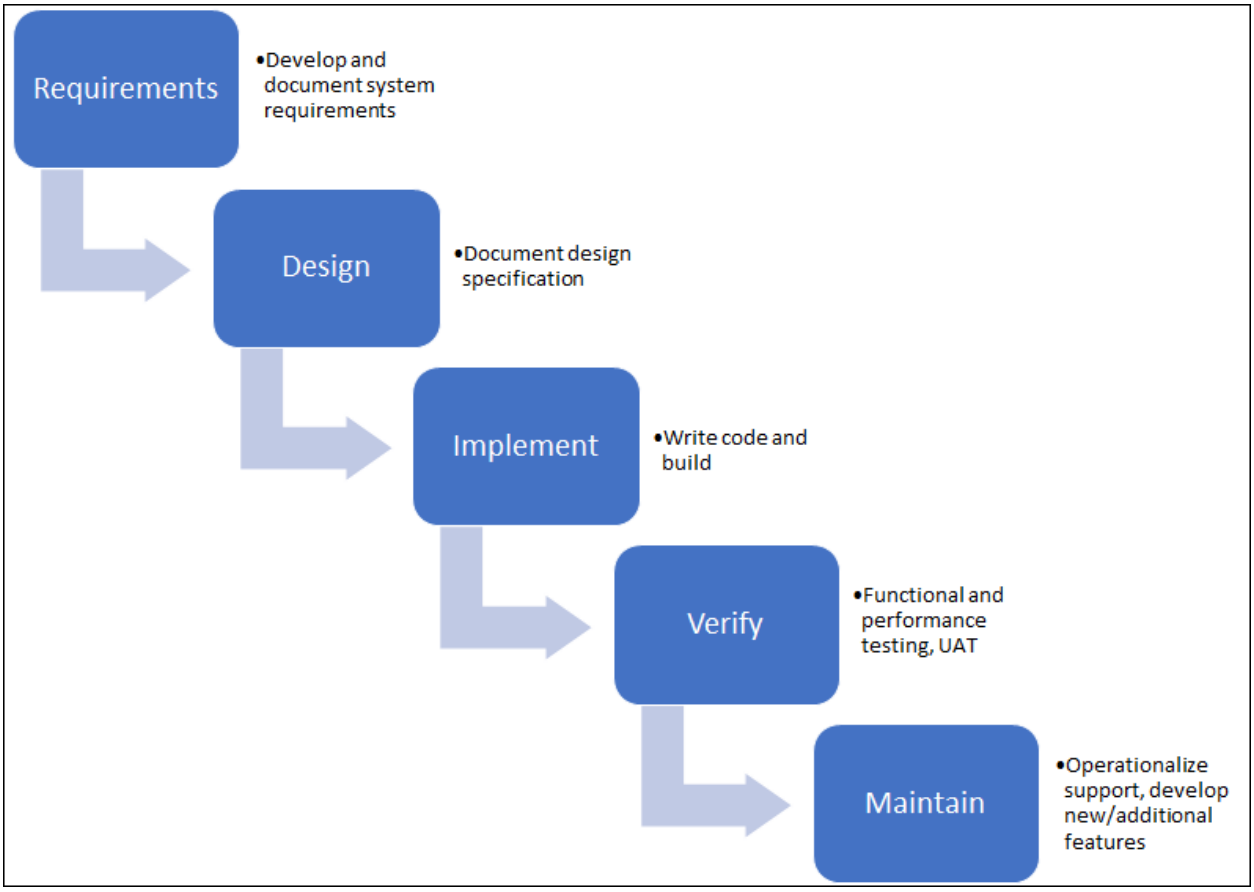


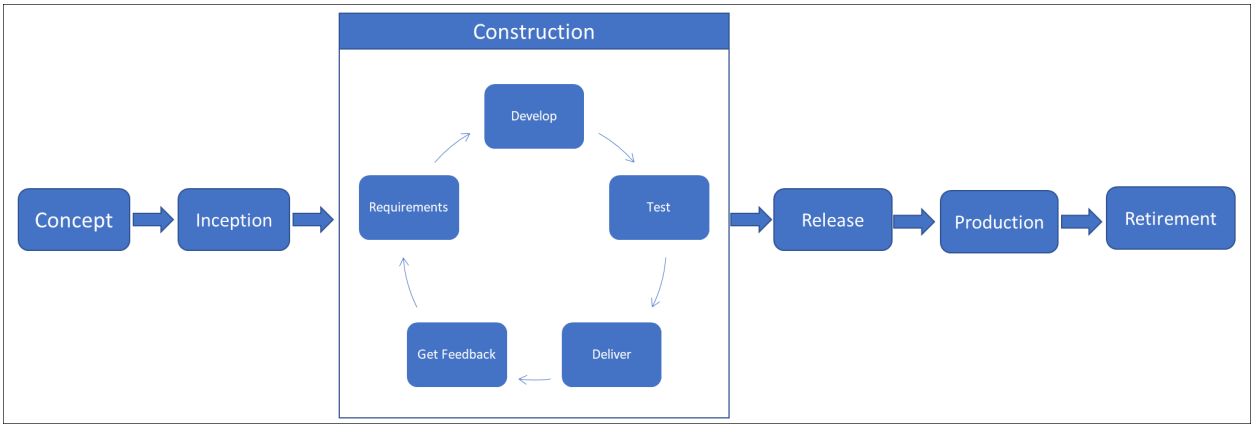
	A	B	D	E	F	K	N
1	Family	Control	Topic	Control/Enhancement Text	Supplemental Guidance	Observation	Maturity
2	AC	1	ACCESS CONTROL POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: 1. Access control policy [Assignment: organization-defined frequency]; and 2. Access control procedures [Assignment: organization-defined frequency].	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations,policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.	In place	4 - Quantitatively Managed

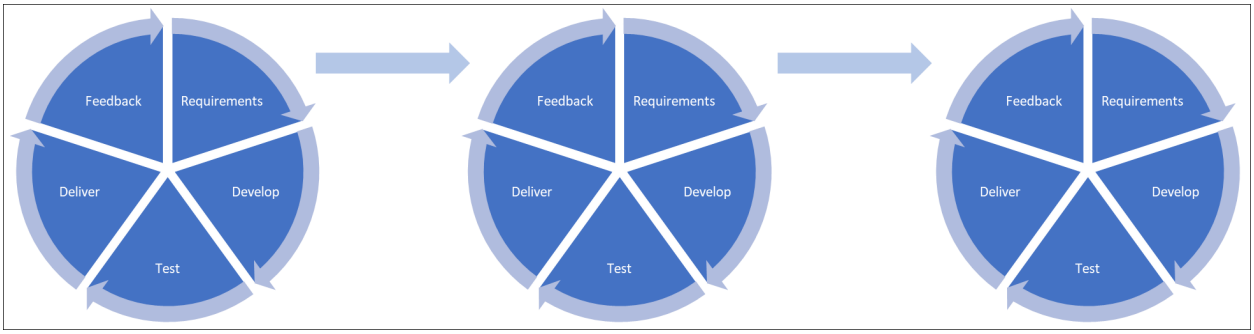

Enter House
Enter through door
Enter through window
Owner allows entry
Force door
Break door
Door left open/unlocked
Use key
Steal key
Pick lock
Force window
Break window
Window left open/unlocked
Social engineer (subterfuge)
Duress/Violence

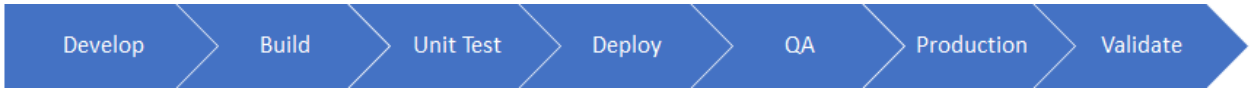

New Threat Model* - Microsoft Threat Modeling Tool
File Edit View Settings Diagram Reports Help DiagramReader
Diagram 1
Account Access Request
HTTP
Browser
Internet Boundary
Web Server
Customer Lookup Request
JDBC
SQL Database
JDBC
Account Data
HTTP
Customer Data Result Set
Threat List
ID Diagram Changed By Last Modified State Title Category Description Justification Interaction Priority
0 Diagram 1 Generated Not Started Spoofing the W Spoofing Web Server ma HTTP High
1 Diagram 1 Generated Not Started Spoofing the B Spoofing Browser may b HTTP High
2 Diagram 1 Generated Not Started Potential Lack o Tampering Data flowing ac HTTP High
3 Diagram 1 Generated Not Started Cross Site Scrip Tampering The web server HTTP High
4 Diagram 1 Generated Not Started Potential Data Repudiation Web Server clai HTTP High
5 Diagram 1 Generated Not Started Data Flow Sniffi Information Dis Data flowing ac HTTP High
6 Diagram 1 Generated Not Started Potential Proce Denial Of Servi Web Server cra HTTP High
7 Diagram 1 Generated Not Started Data Flow HTTP Denial Of Servi An external age HTTP High
8 Diagram 1 Generated Not Started Elevation Using Elevation Of Pri Web Server ma HTTP High
Export Csv
21 Threats Displayed, 21 Total
Threat Properties
No threats are selected
Threat Properties
Notes - no entries

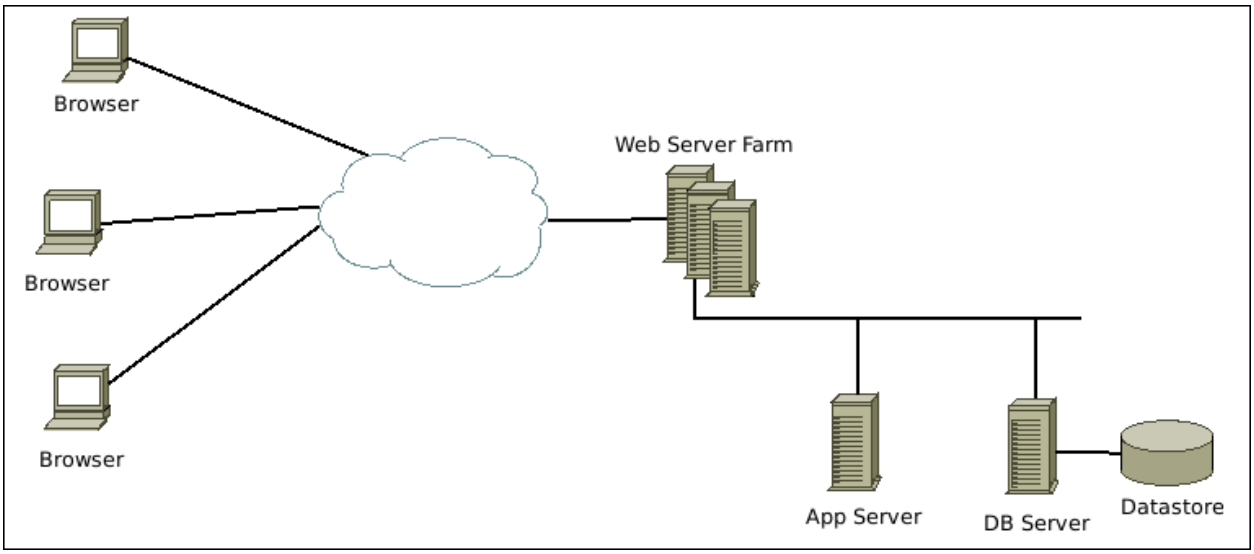
Chapter 6: Building an Architecture – Application Blueprints

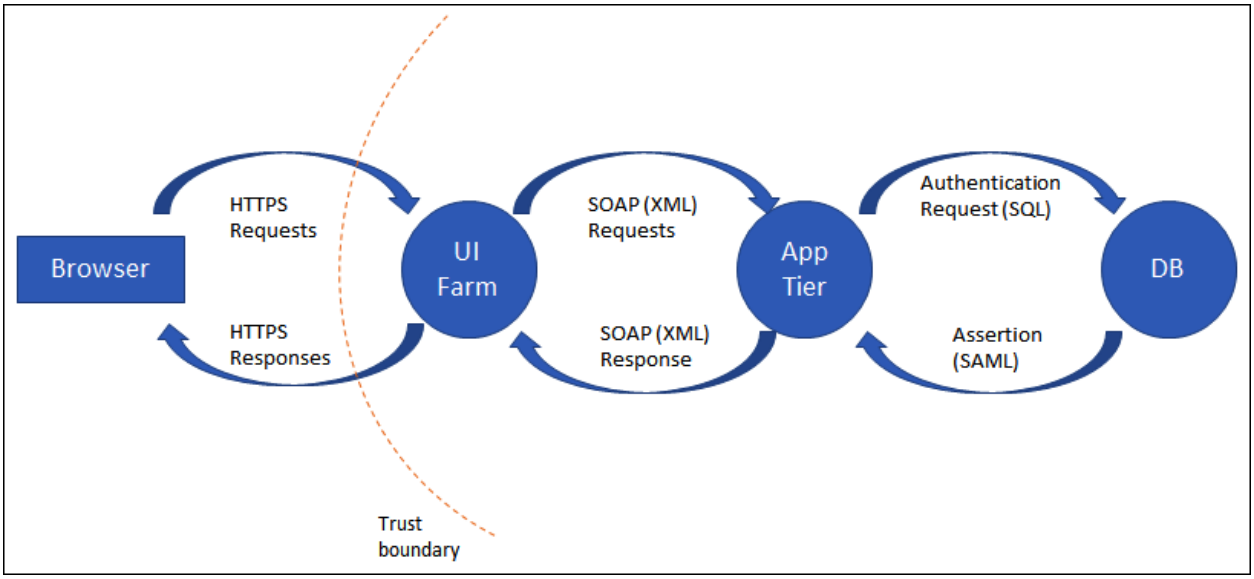





Feedback
Requirements
Deliver
Develop
Test
Feedback
Requirements
Deliver
Develop
Test
Feedback
Requirements
Deliver
Develop
Test

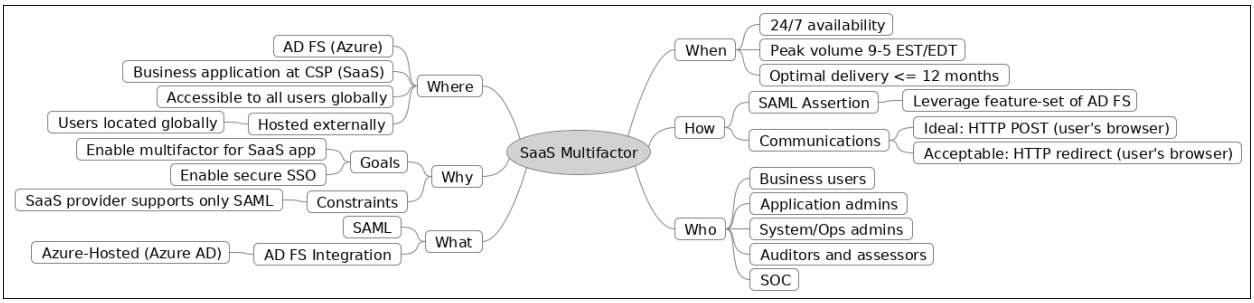

Develop
Build
Unit Test
Deploy
QA
Production
Validate

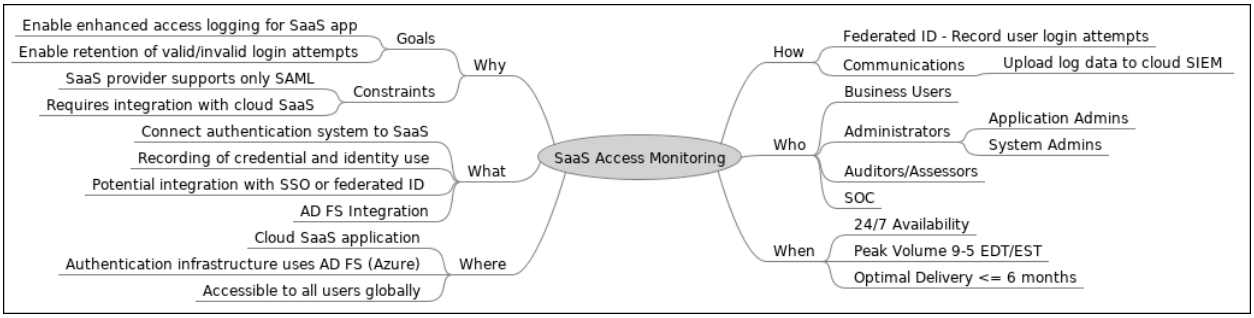

Browser
Browser
Browser
Web Server Farm
App Server
DB Server
Datastore

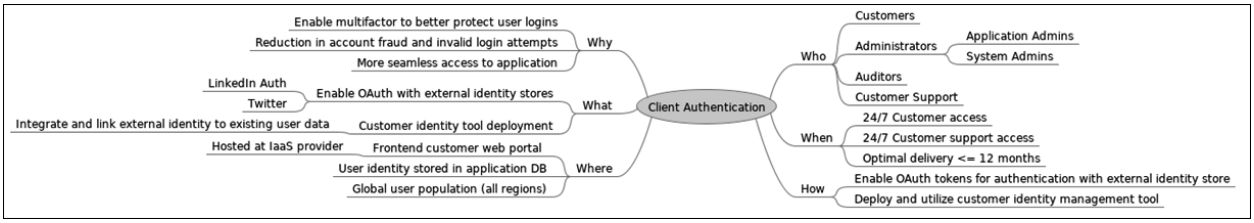

Browser
HTTPS
Requests
HTTPS
Responses
UI
Farm
SOAP (XML)
Requests
SOAP (XML)
Response
App
Tier
Authentication
Request (SQL)
Assertion
(SAML)
DB
Trust
boundary

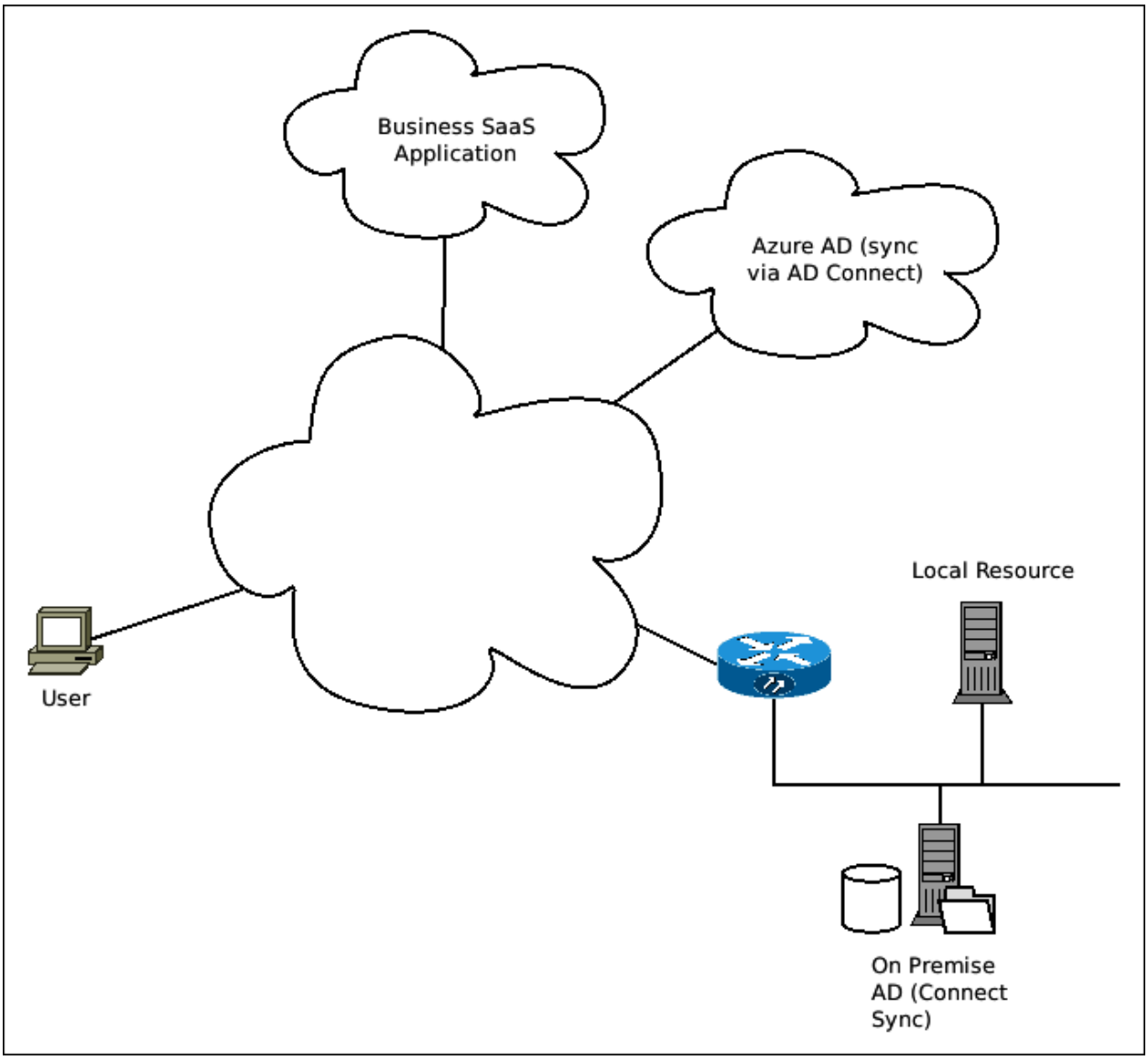
Chapter 7: Execution – Applying Architecture Models

Who	Needs to authenticate business users and application administrators. Needs to provide reporting to internal and external auditors. Needs to provide monitoring information to the security operations center.
What	Needs to support SAML integration with active directory via Active Directory Federation Services (AD FS).
When	Needs to operate at all times, peak times 9AM to 5PM Eastern time, non-peak access 24/7.
Where	AD FS hosted via Azure; business application hosted at cloud services provider.
Why	SaaS service supports only SAML assertions for federation with existing user stores.
How	Federation accomplished via SAML assertion. Communication pathway happens over HTTP POST (ideally) or HTTP redirect binding. Leverages built-in capabilities of SaaS authentication federation model.

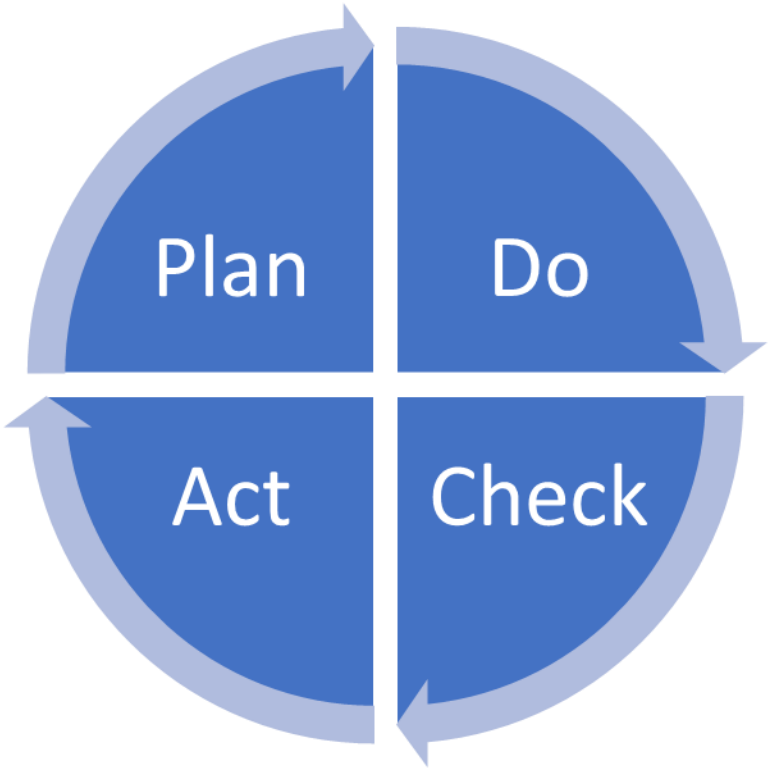







Business SaaS Application
Azure AD (sync via AD Connect)
Local Resource
User
On Premise AD (Connect Sync)

Chapter 8: Execution – Future-Proofing



Chapter 9: Putting It All Together