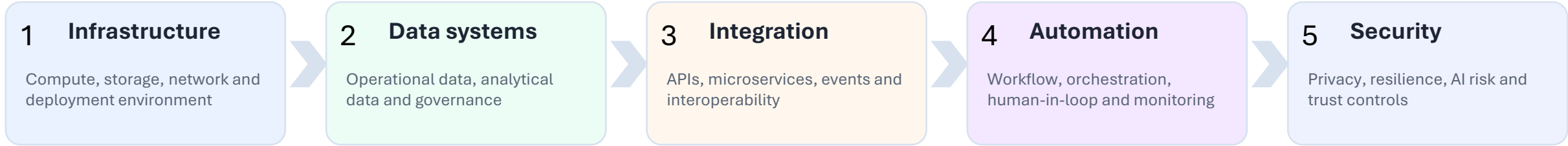


Integration, Automation and Security foundations

Architectural capabilities required to operationalize AI

Leadership with AI – IIT Bombay. Rajendra M Sonar, Ph.D. 

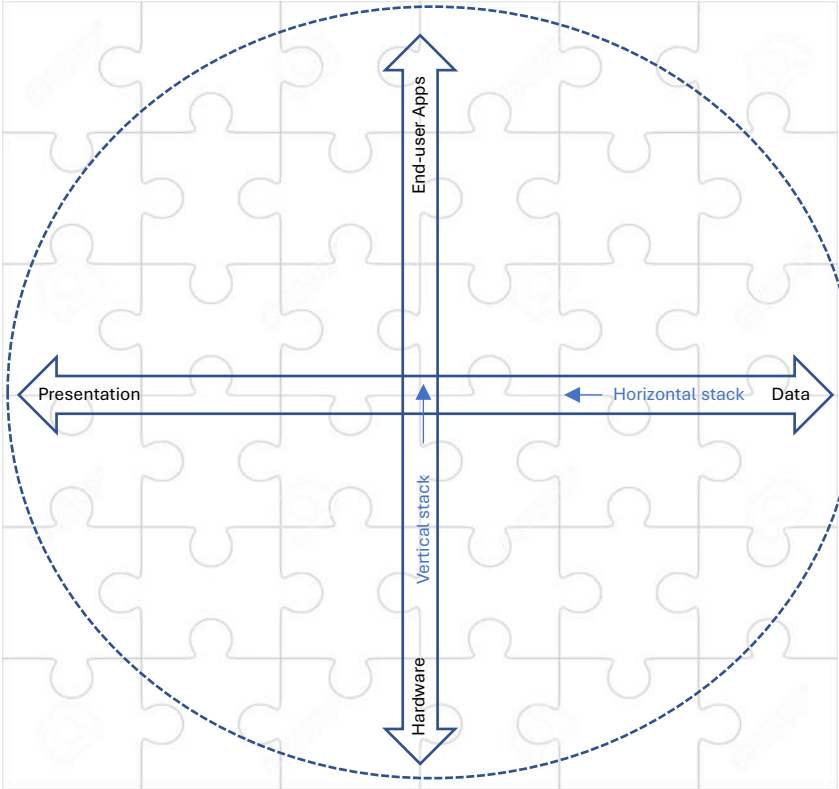
Session Flow: From Architecture to Secure Automation



Core message

AI at scale is a systems-engineering and governance problem, not only a data-science problem.

Complexity of digital systems and technology/software stacks



Open systems and highly distributed systems, networks, Internet, external systems, wireless technologies, Interconnected systems, virtual nature of digital systems etc.



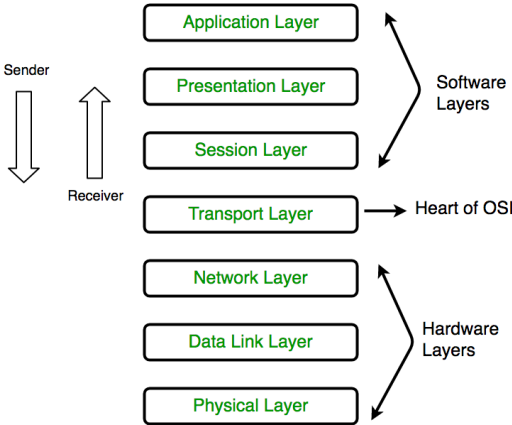
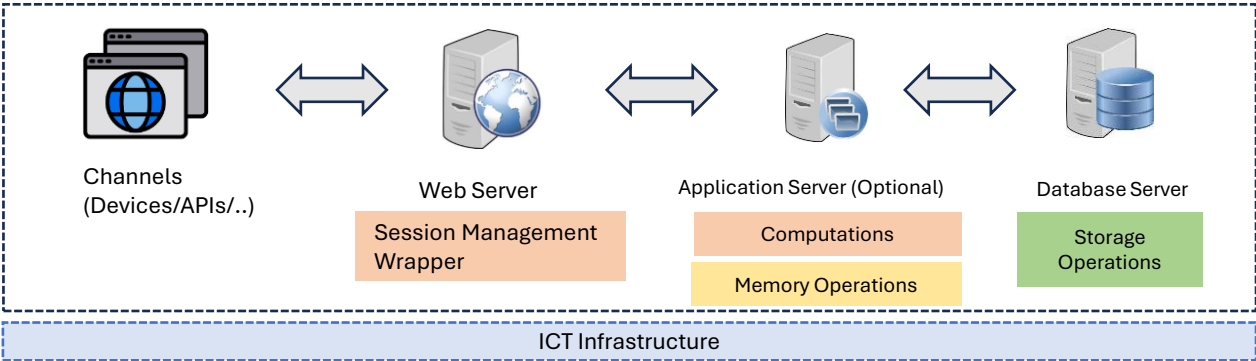
Different types of users

Distributed and loosely coupled (Integration, orchestration mechanism, Networks, Internet, Intranet, Extranet, Cloud etc.)

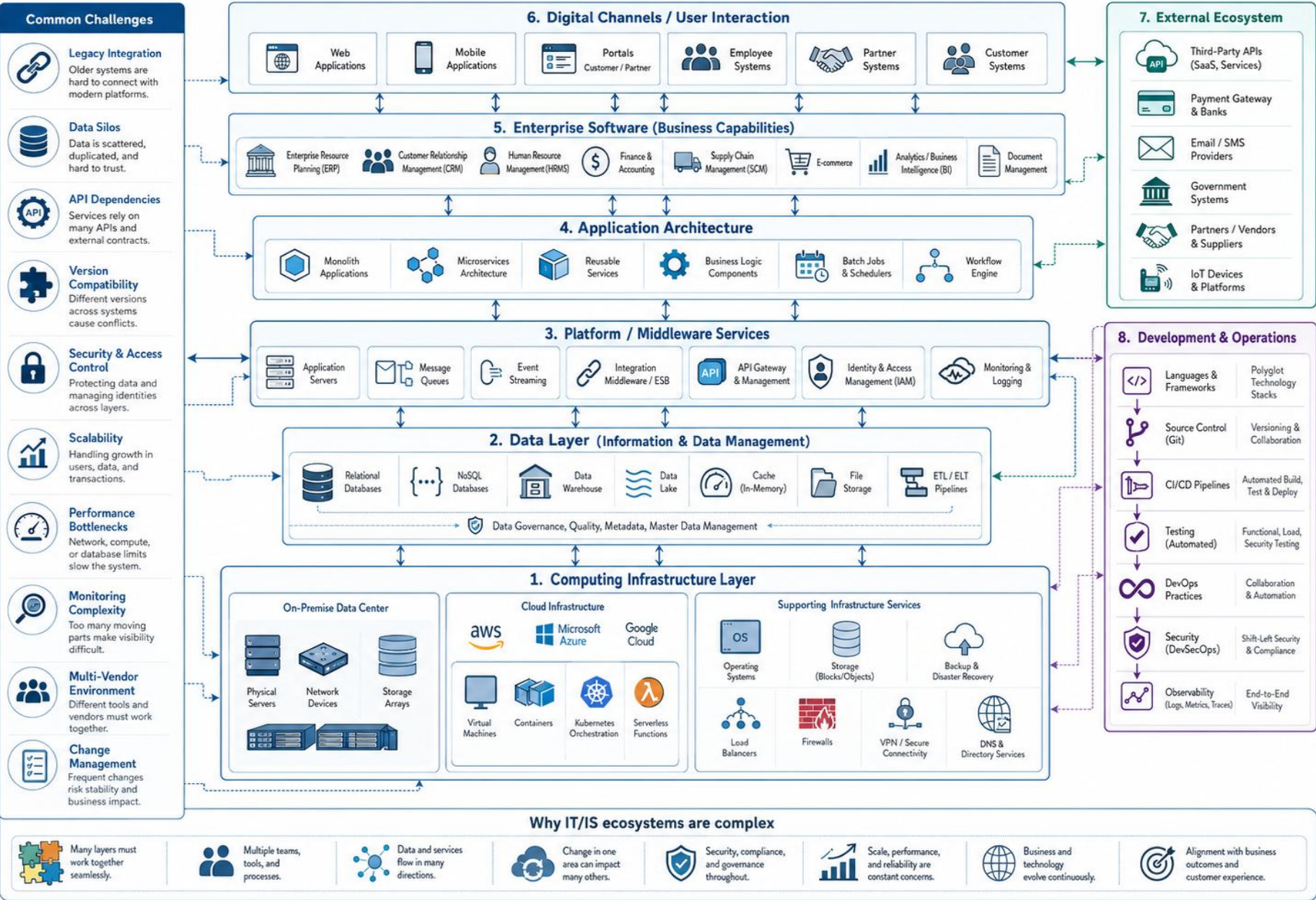
Ownerships are distributed, different licensing policies, virtual or black boxes, no control...

Almost everything is in multiples: H/W, OS, Browsers, back-ends, platforms...

- Interorganizational Systems | Standards | Regulations
- Enterprise Systems
- Domain | Functions | Business Processes | WFs
- Apps | Software | Other Systems
- APIs | Microservices | Components | Hooks
- Platforms | Frameworks | Patterns | Languages
- Back-end Systems (DBMS, Servers: email, CMS, file etc.)
- Browsers | Containers
- Protocols | Communication
- Operating System
- Hardware + Firmware (devices | storage | compute | network)



Complexity of digital systems and technology/software stacks



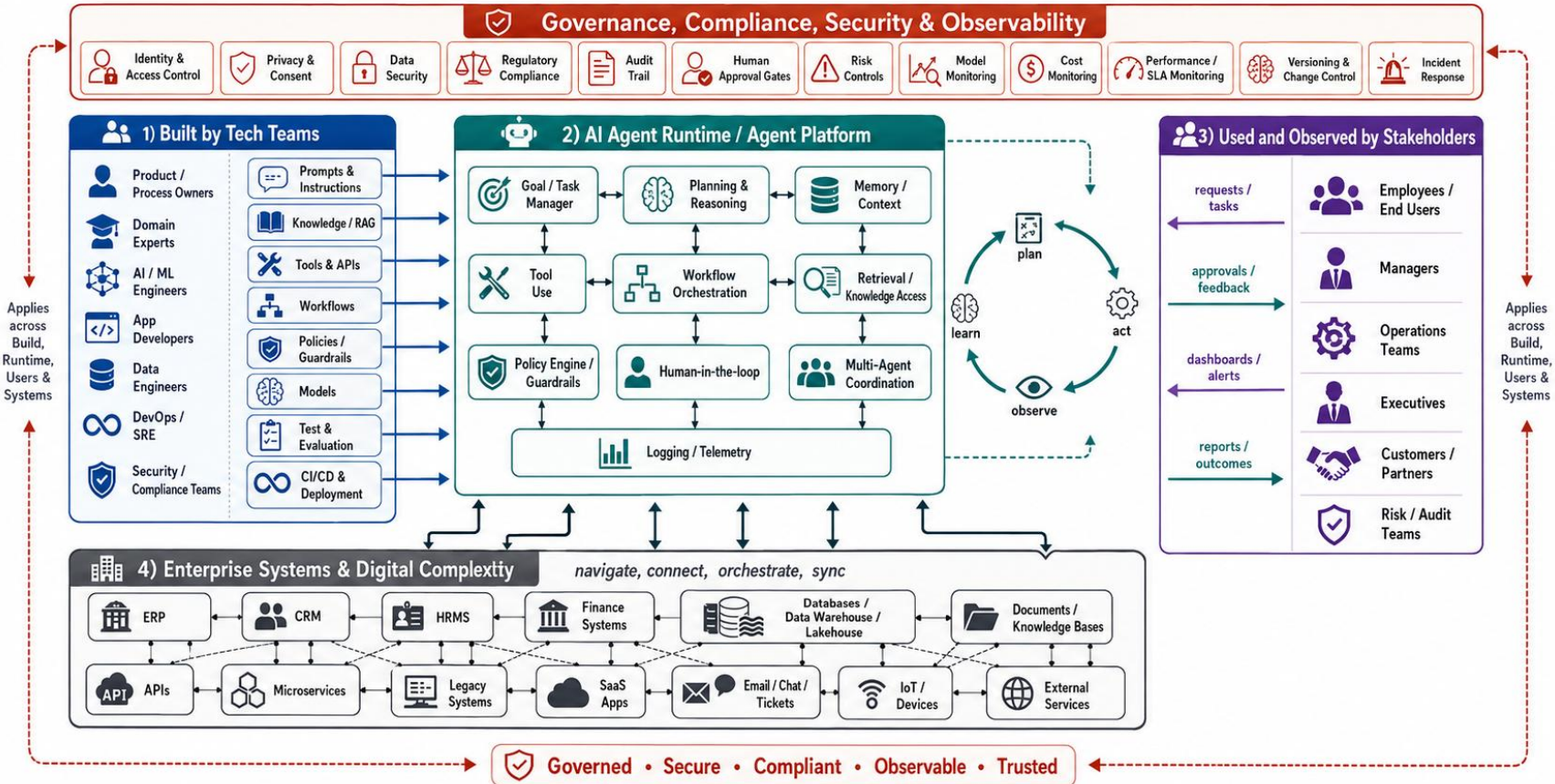
Imagine and think, how AI Agents will be built by tech teams, used and monitored, observed by stakeholders, navigate, connect, orchestrate, sync through complexities of IT systems and at the same time be compliant and governed with all aspects!

Appreciate need of core CS/IT guys, AI engineers, ML developers, security, compliance and domain experts.

Complexity of digital systems and technology/software stacks

Enterprise AI Agents: Build, Use, Monitor, Govern

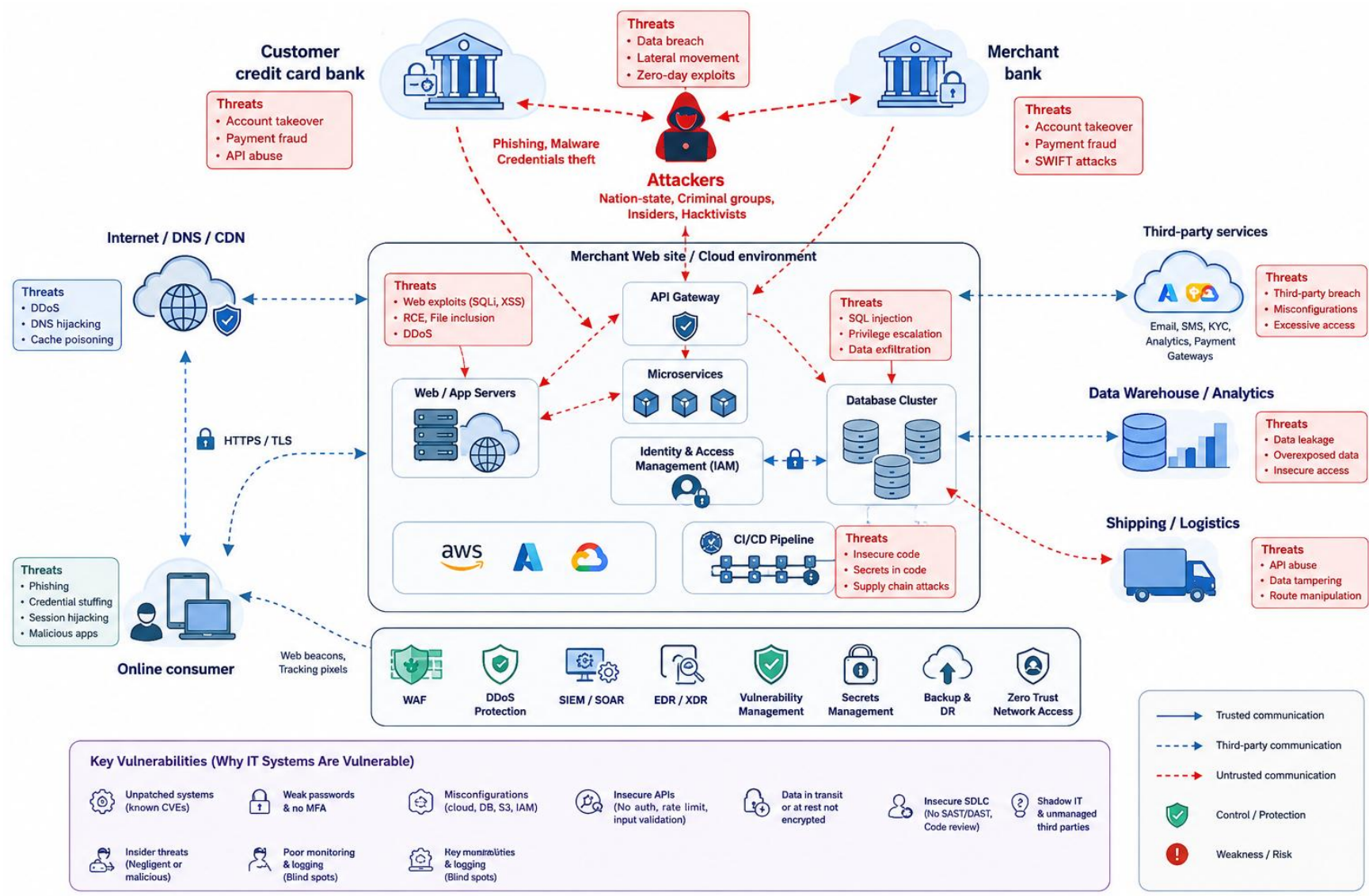
How AI agents are engineered, orchestrated across IT systems, observed by stakeholders, and kept compliant



Imagine and think, how AI Agents will be built by tech teams, used and monitored, observed by stakeholders, navigate, connect, orchestrate, sync through complexities of IT systems and at the same time be compliant and governed with all aspects!

Appreciate need of core CS/IT guys, AI engineers, ML developers, security, compliance and domain experts.

Security primer: complexity of digital systems and technology/software stacks



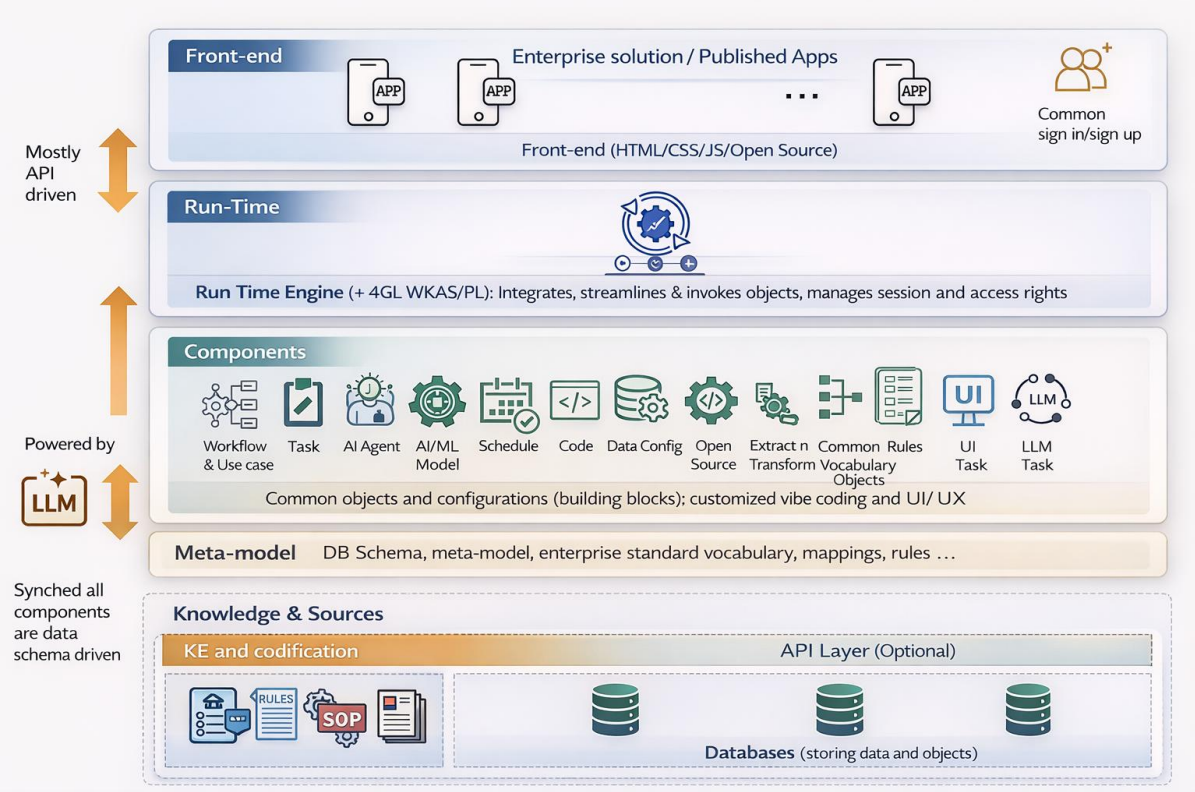
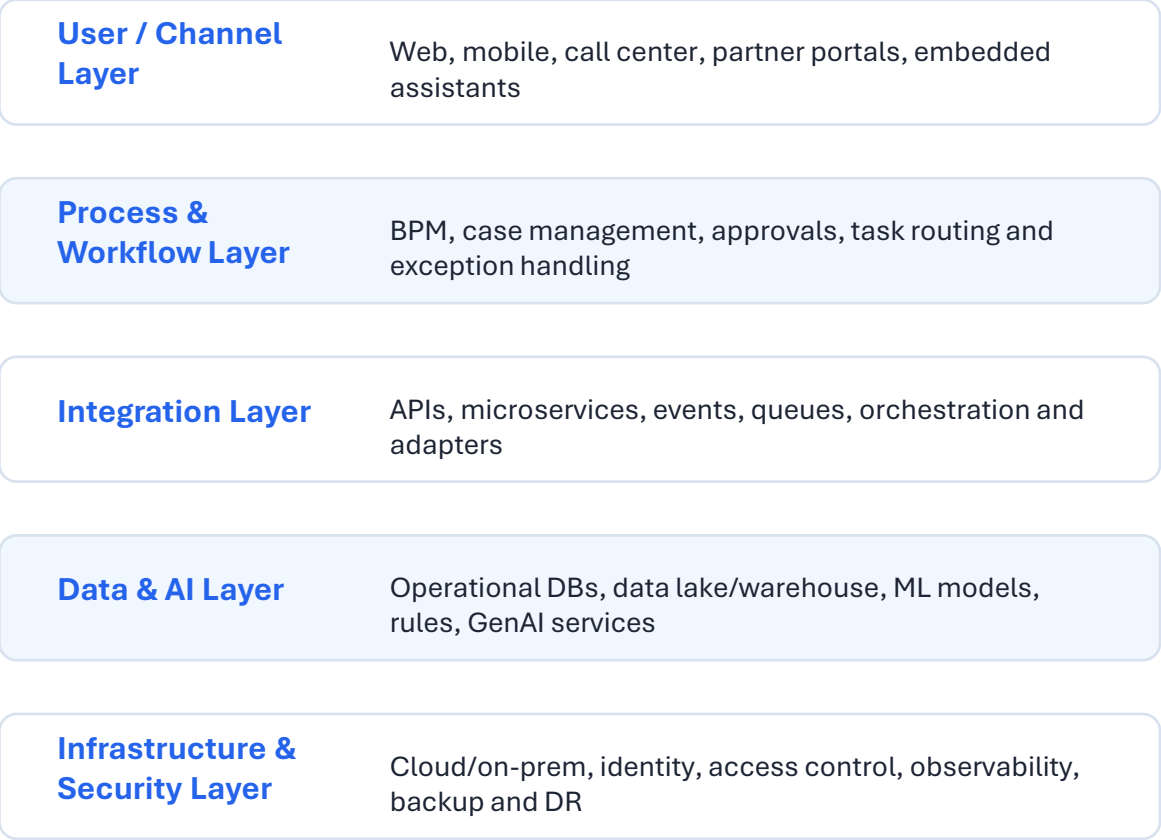
Imagine end-to-end automation using Agentic AI without human intervention!

Security primer: complexity of digital systems and technology/software stacks

Frequently used terms in security domain

IT	Information Technology	DDoS	Distributed Denial of Service	KYC	Know Your Customer	CSPM	Cloud Security Posture Management
DNS	Domain Name System	DoS	Denial of Service	SWIFT	Society for Worldwide Interbank Financial Telecommunication	SCA	Software Composition Analysis
CDN	Content Delivery Network	WAF	Web Application Firewall	AWS	Amazon Web Services	SBOM	Software Bill of Materials
HTTPS	HyperText Transfer Protocol Secure	SIEM	Security Information and Event Management	Azure	Microsoft Azure cloud platform	PKI	Public Key Infrastructure
TLS	Transport Layer Security	SOAR	Security Orchestration, Automation and Response	GCP	Google Cloud Platform	HSM	Hardware Security Module
API	Application Programming Interface	EDR	Endpoint Detection and Response	CVSS	Common Vulnerability Scoring System	PAM	Privileged Access Management
IAM	Identity and Access Management	XDR	Extended Detection and Response	SOC	Security Operations Center	RBAC	Role-Based Access Control
CI/CD	Continuous Integration / Continuous Delivery or Continuous Deployment	DR	Disaster Recovery	VPN	Virtual Private Network	ABAC	Attribute-Based Access Control
DB	Database	MFA	Multi-Factor Authentication	IDS	Intrusion Detection System	SLA	Service Level Agreement
SQL	Structured Query Language	CVE	Common Vulnerabilities and Exposures	IPS	Intrusion Prevention System	SOP	Standard Operating Procedure
XSS	Cross-Site Scripting	SAST	Static Application Security Testing	DLP	Data Loss Prevention	PII	Personally Identifiable Information
RCE	Remote Code Execution	DAST	Dynamic Application Security Testing	MDR	Managed Detection and Response		

Technology Architecture View for AI-Enabled Organizations



A sample architecture diagram

The architecture must allow insight to move safely from data → decision → workflow → audit trail.

Computing Infrastructure: What Leaders Should Understand



Cloud

Elastic capacity, managed services, faster experimentation and scaling.



On-prem / private

Control, compliance, legacy integration and latency-sensitive workloads.



Edge

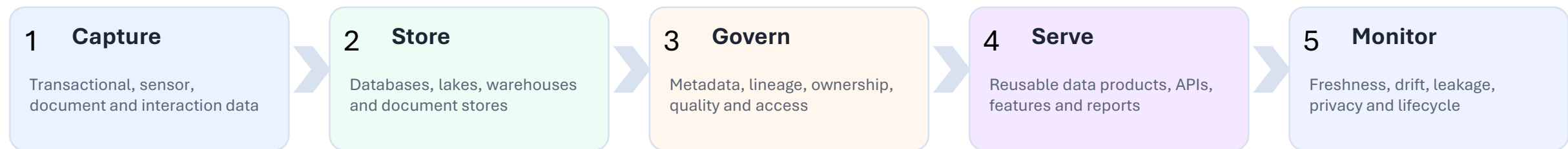
Low-latency processing near devices, plants, vehicles or branches.



Hybrid

Practical enterprise pattern combining cloud, legacy and domain constraints.

Data Management Foundations for AI



AI needs fit-for-purpose data, not just more data.
Operational data and analytical data must be connected with governance.
Data quality issues become AI quality, trust and compliance issues.

APIs, Microservices and Interoperability

API APIs

Standard interfaces for data access, business operations and AI services.

μ Microservices

Smaller deployable services with clear responsibilities and contracts.

EVT Events / queues

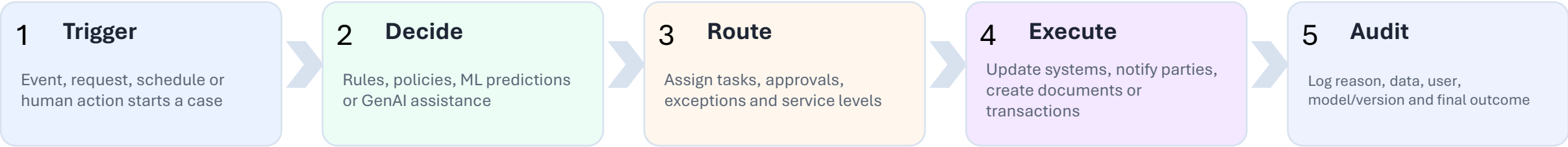
Asynchronous communication for scalable workflows and real-time response.

↔ Interoperability

Common semantics, schemas, identity and integration patterns across systems.

Leadership watch-out: integration complexity is often the hidden cost of AI scaling.

End-to-End Automation: Beyond Task Automation



Automation readiness requires process clarity, clean handoffs, exception design and measurable controls.

AI + Automation: Where Humans Stay in the Loop

H Human approval

High-impact or regulated decisions need accountable review.

E Exception handling

Low-confidence, ambiguous or policy-conflicting cases are escalated.

F Feedback capture

Human corrections become learning signals for data and model improvement.

A Auditability

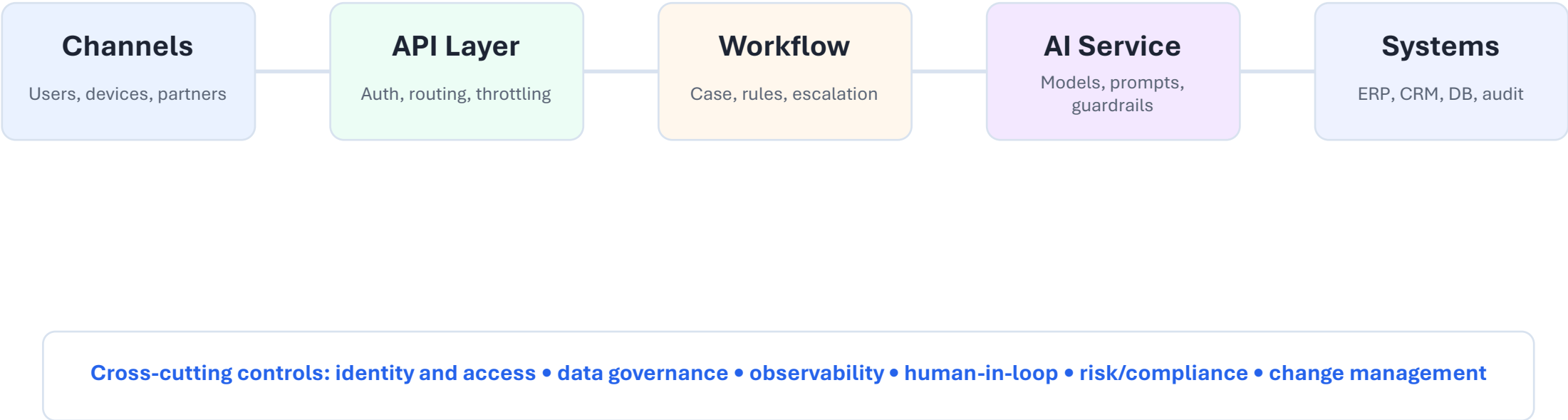
Every automated decision needs traceability and explanation at the right level.

Security, Privacy and Resilience Foundations

- Identity and access management
- Secure APIs and secrets management
- Privacy-by-design and consent controls
- AI-specific risks: prompt injection, data leakage, hallucination and model misuse
- Data classification and encryption
- Logging, monitoring and incident response
- Backup, disaster recovery and business continuity
- Vendor, cloud and third-party risk management

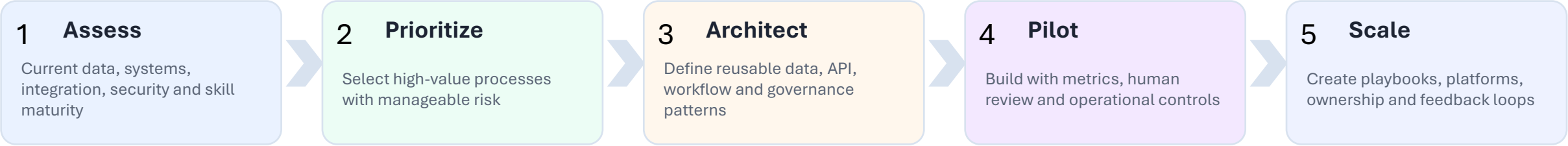
Security is not a final checklist; it must be designed into data, APIs, workflows and AI controls from day one.

Reference Architecture: AI-Enabled Business Process



Use this diagram to ask: where is the AI decision made, where is it recorded, and where can humans override it?

Implementation Roadmap for AI-Ready Foundations



Avoid random pilots. Build repeatable foundations that make the second and third AI use case faster than the first.

Session 2 Takeaways

1 Architecture matters

AI must be connected through a well-designed enterprise architecture.

2 Integration is the scaling lever

APIs, services and events convert AI output into business action.

3 Automation needs controls

Human-in-loop, exception handling and audit trails create responsible automation.

4 Security is foundational

Privacy, resilience and AI risk controls must be designed upfront.