Microsoft

Breaking through with the Cloud in Financial Services

Dave Dadoun, Assistant General Counsel

Challenges and Opportunities

- Regulatory – What is Required?
- Customer – Risk Assurance and Accountability
- Cloud Vendor – Transparency and Oversight
- Third-Parties – Law Enforcement Access

Building a Trusted Cloud

At Microsoft, we never take your trust for granted

- We are serious about our commitment to protect customers in a cloud first world.
- We live by standards and practices designed to earn your confidence.
- We collaborate with industry and regulators to build trust in the cloud ecosystem.

Regulatory Requirements

Understanding the Landscape

Perception:
Regulators won’t allow us to go into public cloud…

No Regulatory Prohibition in Use of Cloud

- There is no blanket regulatory impediment to hosting systems of record in the cloud
- Microsoft has a proven track record in the financial services sector and a sophisticated control environment

Microsoft's Experience in Enabling Cloud Adoption

Europe	**Africa**	**Asia**	**Americas**
Austria	South Africa	Australia	Argentina
Belgium		Hong Kong	Brazil
Denmark		India	Canada
Finland		Indonesia	Chile
France		Japan	Columbia
Hungary		Malaysia New Zealand	Costa Rica
Ireland		Philippines	Ecuador
Italy		Singapore	Mexico
Netherlands		Sri Lanka	Panama
Norway		Thailand	Peru
Portugal		Vietnam	Puerto Rico
Romania			United States
Spain Sweden			Uruguay
Switzerland			
United Kingdom			

Nc

Regulatory Engagement

Customer Requirements

Risk Assurance and Accountability

Risk Factors

- Untrusted environments
- Public cloud environments
- Track records
- Transition in and out arrangements
- Service and control stability
- Assessment of the control environment
- Jurisdictional, contractual or technical considerations

Query

- Control environment instead of identity of tenants
- Scale and sophistication of security investments
- Rigour of risk management practices

The importance of a **relative** risk assessment

- Risk profile of the cloud service you are considering

Compared with

- Risk profile of the status quo (which may be on-premises)
- Risk profile of the other options (which may include hosted private cloud, community cloud)

The Foundations of a Trusted Cloud

Security	Privacy	Compliance	Transparency
Service Provider Reputation and Competence	Limits on Data Use	Confidentiality and Certified Security Standards	Audit & Inspection
Resilience and Business Continuity	Conditions on Subcontracting	Review, Monitoring & Control	Data Location & Transparency
Data Segregation/Isolation	Conditions on Termination	Commercial Commitments	Documents

Cloud Vendors

Transparency and Oversight

What Financial Services Regulators Want

Visibility on the full value chain (with Regulator ability to inspect)

Customer accountability and control over that value chain

Regulator Right to Examine

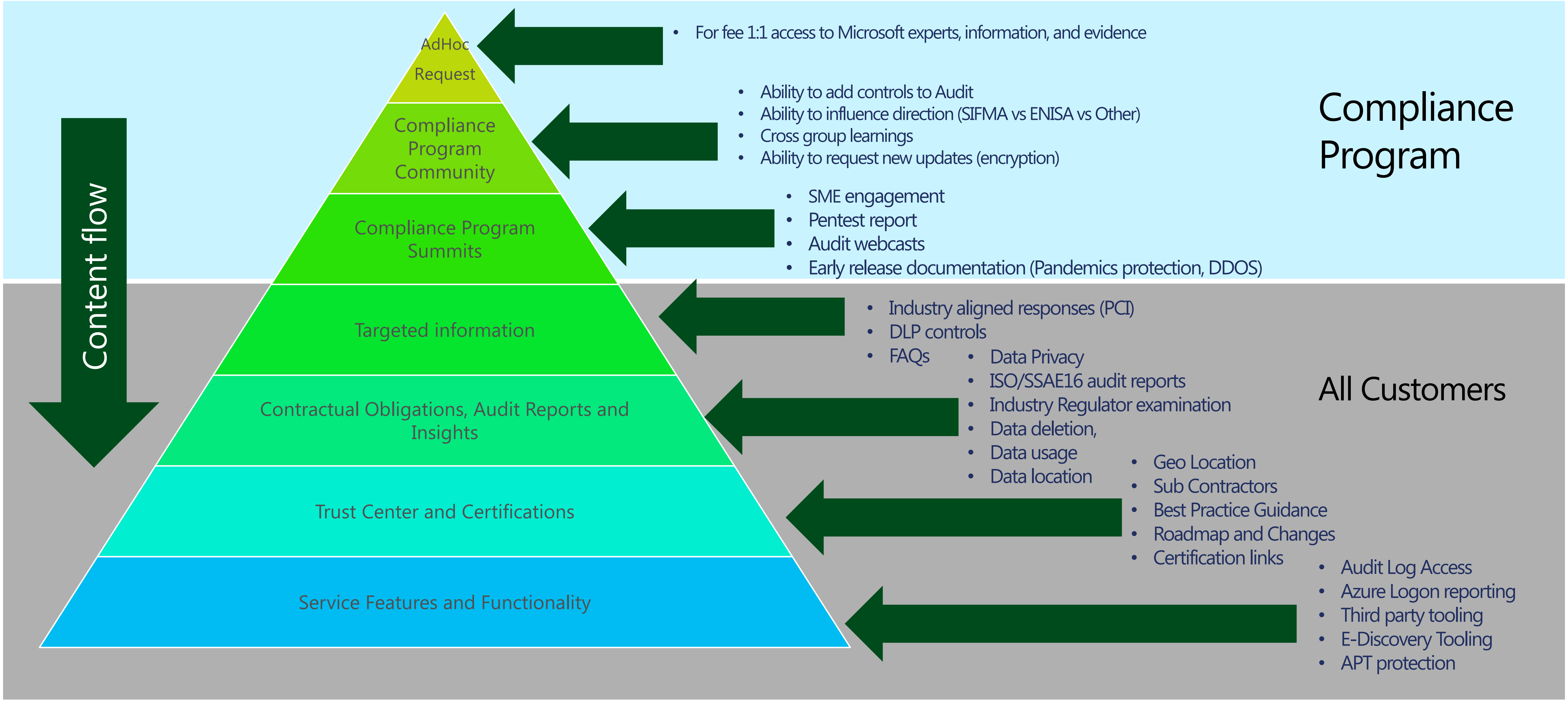
Greater customer oversight of services via Compliance Program

- Access to control framework and services operations data
- Access to security incident reviews and threat evaluations
- Access to Microsoft security experts and external auditors
- Access to penetration testing reports
- Notification of changes that materially impact Microsoft's ability to provide the services

Customer ability to provide suggestions to influence additional controls

Microsoft Standard Financial Services Offering

Enabling Audit at Scale



Third Party Law Enforcement

Balancing Security and Privacy

"In short, when governments seek information from Microsoft relating to customers, we strive to be principled, limited in what we disclose, and committed to transparency."

Brad Smith
General Counsel & Executive Vice President
Microsoft Corporation

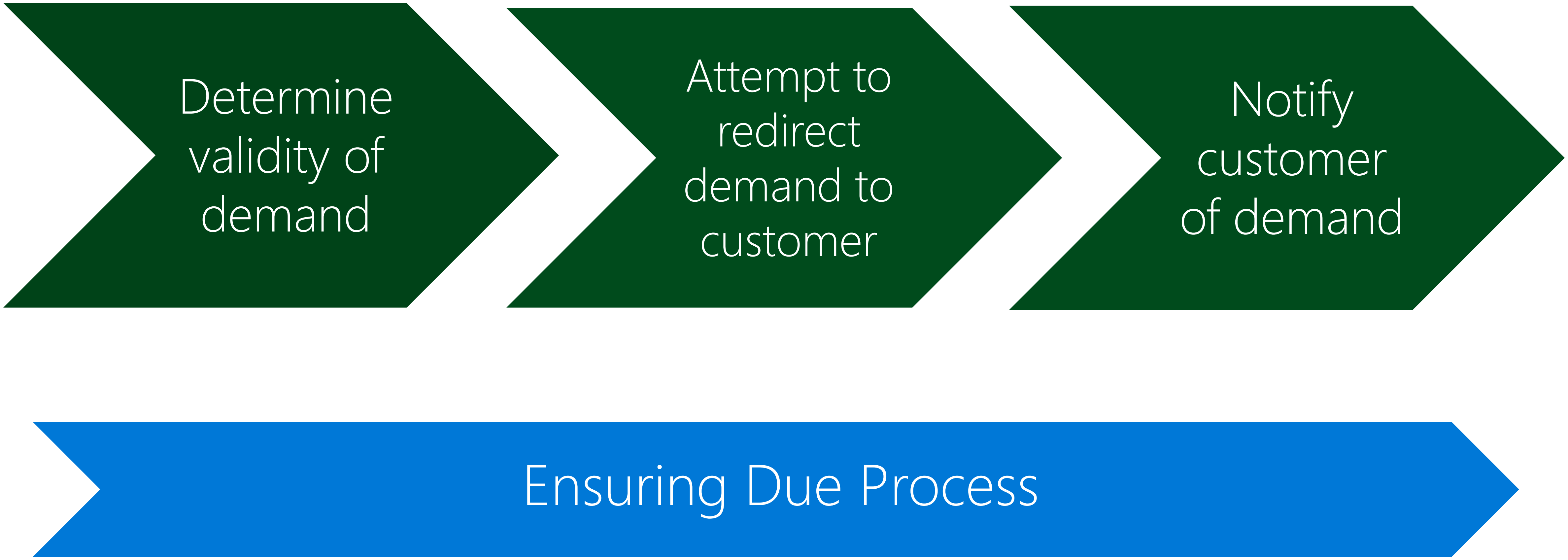
Customer data
≠
Microsoft data

Government demand
↓
Customer

Data access governed by law where it rests

Evolving the law

Microsoft Process for Responding to Government Demands for Customer Data



Microsoft