Windows Azure | Capability Discussion Guide

BUSINESS DRIVER	PHASE 1		PHASE 2		PHASE 3	
	Business Capabilities	Solution Components	Business Capabilities	Solution Components	Business Capabilities	Solution Components
Retain and attract customers with a lean customer support staff	Provide self-managing capability to provision data services for applications throughout the enterprise without adding to the support burden of the IT department	via a highly available, scalable, multiple-tenant storage service in the cloud that includes built-in fault tolerance; and via a simplified process of creating, prototyping, and deploying applications that integrate data across the organization	Provide the ability to build, modify, and distribute scalable applications through a combination of cloud and on-premises resources. Provide the ability to bring ideas to market faster with near-zero capital and operational expenditures	via a cloud-based development, service hosting, and service management environment that provides on-demand computing and storage to host, scale, and manage web applications on the Internet via consumption of computing resources only as needed	Offer a systematic and secure solution that is deployed from the cloud, integrates with on-premises assets, and gives the IT organization oversight and control of distributed data assets along with a consistent development and management experience across the premises and the cloud	via a simple, reliable, flexible, and powerful platform to create web applications and services that support multiple languages and standards and integrate with the existing on-premises environment
Deepen business insights less expensively	Provide the ability to link existing on-premises data stores to cloud-based storage services that support on-demand computing and storage capabilities while ensuring a familiar and consistent application development model	via a familiar application development and relational data model in the cloud that provides connectivity with existing on-premises storage	Provide the ability to create new applications in the cloud without abandoning existing on-premises applications Provide the ability to create new applications in the cloud that can consume data that resides on-site	via bidirectional data synchronization between on-premises and cloud storage via bidirectional data synchronization between cloud applications and on-premises data storage	Extend the availability of on-premises data to allow information to be easily shared with remote offices, mobile workers, and business partners through the cloud from multiple locations, desktop systems, and other devices	via building business data hubs in the cloud, and via a bridge that enables on-premises and off-premises applications to work together
	Provide the ability to expose and consume applications and services over the Internet across firewall, domain, and network boundaries	via secure connectivity between loosely coupled services and applications that enable users to navigate through firewalls or network boundaries and to use a variety of communication patterns	Lower barriers to build composite applications, scalable and custom web applications, and packaged line-of-business applications Provide the ability to consume disparate data sets, imagery, and content in real-time by using virtually any platform, application, or business workflow Provide the ability to easily and flexibly configure users on different identity-management infrastructures while addressing a variety of security needs	via bidirectional communication that is interoperable with existing systems, exposes endpoints easily, supports multiple connection options, and enables publish and subscribe for multicasting via a cloud computing platform that handles storage, delivery, billing, and reporting under a unified provisioning and billing framework via creating user accounts that federate a user’s existing identity management using any directory system or standards-based infrastructure	Provide the ability to secure applications that extend beyond organizational boundaries and exercise complete, customizable control over the level of access that each user and group has within the application	via federated identity and access control through rules-based authorization and flexible standards-based service that supports multiple credentials and parties that rely on it

🟥 🟦 🟧 🟩

Windows Azure | Capability Discussion Guide

Summary Basic Standardized Rationalized Dynamic

			PHASE 1					PHASE 2					PHASE 3				
			B	S	R	D		B	S	R	D		B	S	R	D	
CORE IO	Datacenter Management and Virtualization	Datacenter Management and Virtualization			🟧					🟧						🟩	
		Server Security			🟧					🟧					🟧		
		Networking			🟧					🟧					🟧		
		Storage			🟧						🟩					🟩	
	Device Deployment and Management	Device Management and Virtualization															
		Device Security															
	Identity and Security Services	Identity and Access			🟧					🟧						🟩	
		Information Protection and Control															
	IT Process and Compliance	IT Process and Compliance		🟦						🟧					🟧		
BPIO	Collaboration	Workspaces															
		Portals		🟦					🟦						🟧		
		Social Computing															
		Project Management															
		Information Access															
		Interactive Experience and Navigation															
	Messaging	Messaging															
	Unified Communications	IM/Presence															
		Conferencing															
		Voice															
	Content Creation and Management	Information Management															
		Process Efficiency															
		Compliance															
		Authoring															
		Multi-Device Support															
		Interoperability															
		User Accessibility															
APO	BI and Analytics Platform	Business Intelligence															
		Data Warehouse Management		🟦					🟦						🟧		
		Big Data															
		Information Services and Marketplaces															
	Database and LOB Platform	Transaction Processing															
		Data Management		🟦						🟧					🟧		
		Application Infrastructure			🟧					🟧						🟩	
	Custom Development	Internet Applications															
		Component and Service Composition															
		Enterprise Integration			🟧					🟧					🟧		
		Development Platform			🟧					🟧						🟩	
		Application Lifecycle Management		🟦						🟧					🟧		

Core IO

🟥 Basic 🟦 Standardized 🟧 Rationalized 🟩 Dynamic

		B	S	R	D	PHASE 1	B	S	R	D	PHASE 2	B	S	R	D	PHASE 3
Datacenter Mgt & Virtualization	Datacenter Mgt & Virtualization			🟧		A defined software library exists. Automated build with defined deployment and provisioning processes. Physical and virtual hardware, software, and consumption unit assets are reconciled and reported on demand (manual or automated), and tools and data repository are in place to track and audit assets. Service capacity and resource utilization are monitored continuously; analysis tools are used to predict the impact of proposed changes (software, hardware, usage, and topology); Workloads can be relocated manually. Chargeback is consumption based. The organization actively uses virtualization to consolidate resources for production workloads. Some Production server resources are virtualized. A virtualized server pool is offered as a service. Performance monitoring of physical and virtual hardware with defined SLAs; health monitoring of applications; supported across heterogeneous environments with manual remediation. IT services are audited for compliance based on documented company and industry-standard policies (HIPAA, SOX, and PCI); reports are generated monthly. Services are available during server failure (e.g. server clustering, hot spares, and/or virtualization recovery solution). Process in place to assign costs for static Service allocations back to business groups; based on capacity not usage, or based on show-back reporting.			🟧		Automated build and deployment with consistent provisioning processes integrated with software and configuration library that includes virtual images; on demand reporting; self service portal for IT or end users to deploy. The IT asset life cycle is automated, and managed using policies, procedures, and tools; management of assets and thresholds are based on automated inventory information. Majority of production server resources are virtualized. Resource pooling implementation supports compliance and cost management strategies, such as Auditing and Reporting, Policy Management, Metered Usage, Multi-Tenancy and Process Automation. Performance monitoring of applications as well as physical and virtual hardware pools with enforceable SLAs; Service health monitoring with consistent reporting across heterogeneous environments. Policy enforcement occurs in near real time based on company and industry-standard polices that allow for immediate quarantine of non-compliant systems, and consistent compliance reporting and standards exist across all IT services. There are multiple levels of service availability clustering or load balancing. Virtualization and management is used to dynamically move applications and services when issues arise with datacenter compute, storage and network resources. Charge back based on cost of resources allocated and consumed, charged in aggregated or abstracted units using a defined Service Catalog (e.g., VM months).				🟩	Software and configuration library is maintained at current update levels with version control and auditing on demand. Resource provisioning and deprovisioning occurs dynamically and is elastic. Workloads are relocated dynamically. The organization has a consolidated view and a consolidated management process across heterogeneous virtual environments, including branch offices.
	Server Security			🟧		Malware protection is centrally managed across server operating systems within organizations, including the host firewall. Protection for select mainstream/non-custom applications and services (such as e-mail, collaboration and portal applications, instant messaging), if available, is centrally managed. Integrated perimeter firewall, IPS, Web security, gateway anti-virus, and URL filtering are deployed with support for server and			🟧		Protection is deployed and centrally managed for all applications and services.			🟧		Protection is deployed and centrally managed for all applications and services.

				🟧		domain isolation; network security, alerts, and compliance are integrated with all other tools to provide a comprehensive scorecard view and threat assessment across datacenter, application, organization, and cloud boundaries.			🟧					🟧		
	Networking			🟧		Redundant Domain Name System servers exist to provide fault tolerance. Dynamic Host Configuration Protocol servers are network-aware and with support for auto configuration. Using IPv6 with IPSec for secure private communication over public network.			🟧		Redundant Domain Name System servers exist on a separate network to provide fault tolerance and isolation, including ability to do zone transfer across boundaries.			🟧		Redundant Domain Name System servers exist on a separate network to provide fault tolerance and isolation, including ability to do zone transfer across boundaries.
	Storage			🟧		If a single disk or system component fails, no data is lost but data availability may be interrupted. Actively used data is geographically distributed or replicated to multiple servers; users have seamless and responsive access to most available servers across boundaries even in high-latency environments. Storage is managed and allocated dynamically from a highly available pool of physical space based on capacity required, and within limits set by policy quotas. Critical data is backed up on a schedule across the enterprise; backup copies are stored offsite, with fully tested recovery or failover based on service-level agreements.				🟩	If a storage node fails, data access transparently fails over with no interruption in availability. Storage is managed and allocated dynamically from an elastic pool of storage capacity available across boundaries with automatic capacity expansion within limits set by business policy. Critical data is backed up by taking snapshots using a centralized, application-aware system.				🟩	Users have secure access to actively used data whether or not they are connected to the enterprise network, and can also access data securely from Internet kiosks and Internet-connected devices. Critical data across the enterprise is protected continuously by replicating it at a separate location or by using a cloud-based service; data backups can be recovered by using a self-service recovery process.
DeviceDeployment&Mgt	Device Mgt & Virtualization															
	Device Security															
Identity&Sec	Identity & Access			🟧		To control access, simple provisioning and de-provisioning exists for user accounts, mailboxes, certificates or other multi-factor authentication methods, and machines; access control is role-based. Federation exists for selected applications. For consumer facing applications, federating with public providers (such as Facebook). Password policies are set within a directory service to enable single sign on across boundaries for most applications. Password resets through internal tools or manual processes. There is a centralized group/role based access policy for business			🟧		Centralized IT offering of Federation services. Multiple Federation and trust relations between separate organizations 1 to 1 relationship. Multi-factor and certificate-based authentication are applied in some scenarios, such as remote access across boundaries (such as On Prem and Cloud). Self service password resets supported. A centralized, group/role based access policy is defined for business resources, applications, and information resources, managed through industry accepted processes.				🟩	Centralized IT offering of Federation services that integrates public identities and services. Offers 1 to many collaboration.

uritySvcs				🟧		resources, managed through internal tools or manual processes. A scalable directory that is integrated and automatically synchronizes with all remaining directories across multiple geographies and isolated domains for all applications with connectivity to cloud when applicable.			🟧						🟩	
	Information Protection & Control															
ITProcess&Compliance	IT Process & Compliance		🟦			Each IT service has a formal definition of reliability. Each IT service has a process to manage bug handling and design changes; IT services are tested according to defined test plans based on specifications. IT service release and deployment processes are formally defined and consistently followed. Each IT service provides service-level and operational-level agreements. Monitoring, reporting, and notifications are centralized for protection against malware, protection of information, and identity and access technologies. Risk and vulnerability are formally analyzed across IT services; IT compliance objectives and activities are defined and audited for each IT service.			🟧		Definitions of reliability for IT services are integrated across IT services and enforceable. IT service issues and design changes are tracked by using formal processes; testing is automated where possible. IT service release processes are uniform across IT services; deployment is automated and offers self service where possible; management reviews each service for readiness to release before deployment. Service-level and operational-level agreements are integrated for IT services; management reviews operational health regularly; some tasks are automated. Monitoring and flexible, tenant/service reporting are aggregated across individual areas for protection against malware, protection of information, and identity and access technologies.			🟧		Risk and vulnerability analysis is integrated across all IT services; IT compliance objectives and activities are integrated across IT services and automated where possible; management regularly audits to review policy and compliance.

BPIO 🟥 Basic 🟦 Standardized 🟧 Rationalized 🟩 Dynamic

		B	S	R	D	PHASE 1	B	S	R	D	PHASE 2	B	S	R	D	PHASE 3
Collaboration	Workspaces															
	Portals		🟦			Multiple portals exist; directory services, authentication, and authorization are not uniform across portals, requiring users to sign in multiple times; user management methods are redundant.		🟦			Multiple portals exist; directory services, authentication, and authorization are not uniform across portals, requiring users to sign in multiple times; user management methods are redundant.			🟧		Portals (enterprise, departmental, and personal) are provisioned by IT and are deployed on a single productivity infrastructure; governance policies are fully in place, including single sign-on supported by uniform directory services.
	Social Computing															
	Project Mgt															
	Information Access															
	Interactive Experience & Navigation															
Messaging	Messaging															
Unified Communications	IM/Presence															
	Conferencing															
	Voice															
Conten	Information Mgt															
	Process Efficiency															
	Compliance															

t Creation and Management	Authoring															
	Multi-Device Support															
	Interoperability															
	User Accessibility															

APO 🟥 Basic 🟦 Standardized 🟧 Rationalized 🟩 Dynamic

		B	S	R	D	PHASE 1	B	S	R	D	PHASE 2	B	S	R	D	PHASE 3
BI & Analytics Platform	Business Intelligence															
	Data Warehouse Mgt		🟦			An IT-managed BI environment is in place and applications at the department level integrate with departmental data marts. IT designs, implements, and manages data schemas that are optimized for localized self-service reporting and analysis tools.		🟦			An IT-managed BI environment and applications at the department level are aligned with the enterprise data warehouse (EDW) environment and applications. IT proactively builds, maintains, and manages key reports and analysis models that are used regularly across the business. IT designs, implements, and manages semantic models (such as OLAP) and data schemas optimized for managed and self-service reporting and analysis.			🟧		An IT-managed BI environment and applications at the department level are aligned with the enterprise data warehouse (EDW) environment and applications. IT proactively builds, maintains, and manages key reports and analysis models that are used regularly across the business. IT designs, implements, and manages semantic models (such as OLAP) and data schemas optimized for managed and self-service reporting and analysis.
	Big Data															
	Information Services & Marketplaces															
Database & L	Transaction Processing															
	Data Management		🟦			Key high-value data has associated formal data management policies and processes. Data governance may be recognized on a siloed basis, but not as a corporate discipline. Data and asset inventories and dependency relationships are manually documented periodically. Access policies for data and objects in databases are defined but not centralized, and do not reference data classifications. Administrative tasks are still performed using an over-privileged account. Security management is performed on a server-by-server basis. Systems are in place for retention backup. Organizational/departmental policies exist for how long items are stored and what is stored.			🟧		Data governance with documented, standardized policies and processes are established and automated for maintaining data consistency and security, but not necessarily optimized. Data access controls are consistently implemented and applied based on data classification. Centrally administered cryptography is used and audited for protection of data-at-rest and data-in-transit. A self-service interface exists for DBAs and/or authorized users to manage security. An information asset inventory and relationship map is able to predict impacts of changes in some areas. Metadata and taxonomies are defined, implemented, and formally managed in one or more repositories with more reliance upon policy-based management to ensure proper configuration and adherence to policies. Business has begun to consolidate data, management plans, and policies for consistency across information stores.			🟧		Data governance with documented, standardized policies and processes are established and automated for maintaining data consistency and security, but not necessarily optimized. Data access controls are consistently implemented and applied based on data classification. Centrally administered cryptography is used and audited for protection of data-at-rest and data-in-transit. A self-service interface exists for DBAs and/or authorized users to manage security. An information asset inventory and relationship map is able to predict impacts of changes in some areas. Metadata and taxonomies are defined, implemented, and formally managed in one or more repositories with more reliance upon policy-based management to ensure proper configuration and adherence to policies. Business has begun to consolidate data, management plans, and policies for consistency across information stores.

	Application Infrastructure			🟧		Application messaging services used by development are aligned with standard application operating environments. Development and operations teams have the skills required to effectively and consistently make use of these technologies. Limited application component and service reuse strategies exist at the departmental or project level. Orchestration and workflow between applications is typically implemented via custom integrations. Applications are beginning to adopt web services or other standards implemented in operating environments to allow application components and common application services to interoperate as needed. Common application services and middleware component frameworks are selected jointly by development and operations teams as part of the application life-cycle management process. A range of application services and infrastructure is provided across operating environments with central governance. A central engineering practices group co-sponsored by development and operations has formed and is providing valuable guidance to application development teams. Application developers consistently build applications using these application frameworks, so hosting, application services requirements, and management are predictable. Operating systems provide support for multiple application frameworks. Applications' deployment standards are consistently followed. A consistent platform for running and managing applications is implemented, and applications are designed with consistent approaches to health monitoring. Operations proactively monitors applications and back-end services using a shared thresholds/alerting infrastructure, and a centralized management tool and/or self-service interface is used to manage applications, services, and physical and virtual assets. Application and service monitoring data may be rendered on process performance dashboards.			🟧		A common application messaging services infrastructure is in place and well managed for larger mission-critical applications.				🟩	Business processes follow a model-driven, dynamic approach. IT manages a SOA-based application infrastructure, comprised of LOB back ends and composite applications that extend them and has complete monitoring of integration scenarios across the cloud and on-premises applications. Use of standard application services supported by the operating application infrastructure environment is maximized. Engineering of infrastructure, shared application services, and application frameworks is performed jointly by development and operations teams, resulting in complete symmetry between development and operating environments. Many application characteristics can be modified by changing application configuration instead of code. Deployment of applications is simplified, consistent, and supported by automation. On-demand capabilities exist to add/change/remove application components without risk of downtime. Application blueprints do not have physical dependencies. Application and cross-application end-to-end process health management is proactive, with sophisticated SLAs and alerting structures in place.
Cust	Internet Applications															

omDevelopment	Component & Service Composition															
	Enterprise Integration			🟧		Use of standardized processes for data integration is at the project level and technologies are used to improve back-end integration. The business leverages an integration broker running on-premises to connect to cloud applications using adapters. Application integrations leverage standard application messaging protocols and infrastructure to connect various applications running on-premises and in the cloud, connecting mission-critical data and transactions across enterprise applications. Centralized data integration strategies and tools are used across the enterprise.			🟧		Applications leverage an application communication infrastructure deployed in operations that is actively managed and has dynamic routing capabilities.			🟧		Applications leverage an application communication infrastructure deployed in operations that is actively managed and has dynamic routing capabilities.
	Development Platform			🟧		The organization has selected and implemented a common set of frameworks for major application development and operating environment needs. Developer skill and use of standard frameworks is consistent. A central architecture and engineering practices group has formed with the participation of development and operations teams, and provides valuable guidance to development teams. A standard set of tools and common development approaches are used across multiple development teams in the organization.			🟧		Developed applications extend line-of-business (LOB) systems (at UX level and mid-tier), extending LOB business logic. IT manages a service-based infrastructure of composite applications that connect and surface best-of-breed LOB systems.				🟩	Use of standard application services supported by the operating application infrastructure environment is maximized. Architectural layering is enforced as part of code delivery and build automation. Engineering of infrastructure and central application services is performed jointly by development and operations teams, resulting in complete symmetry between development and operating environments. Development work management tools are integrated with operations incident management systems.
	Application Lifecycle Mgt		🟦			Work-breakdown structures map estimated work to business value. Rudimentary metrics are used to manage project progress. Project managers aggregate data from standard status updates. Effective change management processes are in place. Testing has test harnesses and some automation, formal unit testing with good code coverage, and defined test strategy and processes. Explicit use of code quality tools typically occurs at the end of the development cycle. Processes are defined for debugging			🟧		Consistent, iterative, well-documented, and cross-functional processes exist across the application life cycle. Project estimates consider historical data. High transparency exists within self-directed teams, cross-team transparency, and stakeholder engagement. Project managers track status via centralized tools. Issue tracking is well integrated with change management. Test-driven development is accepted. Applications are designed for testability, with architectural and layer verification and validation. Agile testing			🟧		Consistent, iterative, well-documented, and cross-functional processes exist across the application life cycle. Project estimates consider historical data. High transparency exists within self-directed teams, cross-team transparency, and stakeholder engagement. Project managers track status via centralized tools. Issue tracking is well integrated with change management. Test-driven development is accepted. Applications are designed for testability, with architectural and layer verification and validation. Agile testing

			🟦			production defects and incidents, with a standard set of defect artifacts.			🟧		is integrated tightly with agile development. Users and stakeholders are engaged on an ad hoc basis. Unit testing, static analysis, and profiling are used regularly. An integrated platform exists between development and operations for application monitoring, incident reporting and management, actionable defect/incident data from monitored applications, communication through support to development teams, and ubiquitous visibility into issue resolution status.			🟧		is integrated tightly with agile development. Users and stakeholders are engaged on an ad hoc basis. Unit testing, static analysis, and profiling are used regularly. An integrated platform exists between development and operations for application monitoring, incident reporting and management, actionable defect/incident data from monitored applications, communication through support to development teams, and ubiquitous visibility into issue resolution status.

Windows Azure | Capability Discussion Guide

Product Recommendations

Core IO 🟥 Basic 🟦 Standardized 🟧 Rationalized 🟩 Dynamic

		B	S	R	D	PHASE 1	B	S	R	D	PHASE 2	B	S	R	D	PHASE 3
DatacenterMgt&Virtualization	Datacenter Mgt & Virtualization			🟧		Compliance Management Libraries 2.0; Data Classification Toolkit; Hyper-V Server 2008 R2; IT Governance, Risk and Compliance process management pack 2.0; Microsoft Assessment and Planning Toolkit 6.5; Microsoft Deployment Toolkit 2012; Microsoft Software Inventory Analyzer 5.1; Security Compliance Management Toolkit; Security Compliance Manager 2.x; Software Asset Management; System Center 2012 Configuration Manager; System Center 2012 Operations Manager; System Center 2012 Orchestrator; System Center 2012 Service Manager; System Center 2012 Virtual Machine Manager; Windows Automated Installation Kit; Windows Azure; Windows Server 2012			🟧		Compliance Management Libraries 2.0; Data Classification Toolkit; Hyper-V Server 2008 R2; IT Governance, Risk and Compliance process management pack 2.0; Microsoft Deployment Toolkit 2012; Security Compliance Manager 2.x; Software Asset Management; System Center 2012 App Controller; System Center 2012 Configuration Manager; System Center 2012 Operations Manager; System Center 2012 Orchestrator; System Center 2012 Service Manager; System Center 2012 Virtual Machine Manager; System Center Virtual Machine Manager Self Service Portal 2.0; Windows Automated Installation Kit; Windows Azure; Windows Server 2012				🟩	Compliance Management Libraries 2.0; Data Classification Toolkit;Hyper-V Server 2008 R2; IT Governance, Risk and Compliance process management pack 2.0; Microsoft Deployment Toolkit 2012; Security Compliance Manager 2.x; Software Asset Management; System Center 2012 App Controller; System Center 2012 Configuration Manager; System Center 2012 Operations Manager; System Center 2012 Orchestrator; System Center 2012 Service Manager; System Center 2012 Virtual Machine Manager; System Center Virtual Machine Manager Self Service Portal 2.0; Windows Azure; Windows Server 2012
	Server Security			🟧		Forefront Threat Management Gateway 2010; Forefront Unified Access Gateway 2010; System Center 2012 Endpoint Protection; Windows Azure; Windows Server 2012			🟧		Forefront Protection 2010 for SharePoint; Forefront Threat Management Gateway 2010; Forefront Unified Access Gateway 2010; System Center 2012 Endpoint Protection; Windows Azure; Windows Server 2012			🟧		Forefront Protection 2010 for SharePoint; Forefront Threat Management Gateway 2010; Forefront Unified Access Gateway 2010; System Center 2012 Endpoint Protection; Windows Azure; Windows Server 2012
	Networking			🟧		Windows Azure; Windows Server 2012			🟧		Windows Azure; Windows Server 2012			🟧		Windows Azure; Windows Server 2012
	Storage			🟧		Microsoft Online Backup Service; System Center 2012 Data Protection Manager; System Center 2012 Operations Manager; System Center 2012 Virtual Machine Manager; Windows 8; Windows Azure; Windows Server 2012; Windows Storage Server 2008 R2				🟩	System Center 2012 Data Protection Manager; System Center 2012 Operations Manager; System Center 2012 Virtual Machine Manager; Windows 8; Windows Azure; Windows Server 2012; Windows Storage Server 2008 R2				🟩	Forefront Threat Management Gateway 2010; Forefront Unified Access Gateway 2010; System Center 2012 Data Protection Manager; System Center 2012 Operations Manager; System Center 2012 Virtual Machine Manager; Windows 8; Windows Azure; Windows Server 2012; Windows Storage Server 2008 R2
DeviceDeployme	Device Mgt & Virtualization															
	Device Security															

nt & Mgt																
Identity & Security Svcs	Identity & Access			🟧		Forefront Identity Manager 2010 R2; Hyper-V Server 2008 R2; Windows Azure; Windows Server 2012			🟧		Forefront Identity Manager 2010 R2; Hyper-V Server 2008 R2; Windows 8; Windows Azure; Windows Server 2012				🟩	Forefront Identity Manager 2010 R2; Hyper-V Server 2008 R2; Windows 8; Windows Azure; Windows Azure Platform; Windows Server 2012
	Information Protection & Control															
IT Process & Compliance	IT Process & Compliance		🟦			Forefront Threat Management Gateway 2010; Hyper-V Server 2008 R2; Microsoft Security Assessment Tool; System Center 2012 Configuration Manager; System Center 2012 Data Protection Manager; System Center 2012 Endpoint Protection; System Center 2012 Operations Manager; System Center 2012 Orchestrator; System Center 2012 Service Manager; System Center 2012 Virtual Machine Manager; Windows Server 2012			🟧		Forefront Threat Management Gateway 2010; Hyper-V Server 2008 R2; Microsoft Security Assessment Tool; SharePoint 2010; System Center 2012 App Controller; System Center 2012 Configuration Manager; System Center 2012 Data Protection Manager; System Center 2012 Endpoint Protection; System Center 2012 Operations Manager; System Center 2012 Orchestrator; System Center 2012 Service Manager; System Center 2012 Virtual Machine Manager; Visio Professional 2010; Windows Server 2012			🟧		Forefront Threat Management Gateway 2010; Hyper-V Server 2008 R2; Microsoft Security Assessment Tool; SharePoint 2010; System Center 2012 App Controller; System Center 2012 Configuration Manager; System Center 2012 Data Protection Manager; System Center 2012 Endpoint Protection; System Center 2012 Operations Manager; System Center 2012 Orchestrator; System Center 2012 Service Manager; System Center 2012 Virtual Machine Manager; Visio Professional 2010; Windows Server 2012

Windows Azure | Capability Discussion Guide

BPIO 🟥 Basic 🟦 Standardized 🟧 Rationalized 🟩 Dynamic

		B	S	R	D	PHASE 1	B	S	R	D	PHASE 2	B	S	R	D	PHASE 3
Collaboration	Workspaces															
	Portals		🟦			Office 365; SharePoint Online; SharePoint Server 2010		🟦			Office 365; SharePoint Online; SharePoint Server 2010			🟧		Office 365; SharePoint Online; SharePoint Server 2010
	Social Computing															
	Project Mgt															
	Information Access															
	Interactive Experience & Navigation															
Messaging	Messaging															
UnifiedCommunications	IM/Presence															
	Conferencing															
	Voice															
ContentC	Information Mgt															
	Process Efficiency															
	Compliance															

reation and Management	Authoring													
	Multi-Device Support													
	Interoperability													
	User Accessibility													

APO 🟥 Basic 🟦 Standardized 🟧 Rationalized 🟩 Dynamic

		B	S	R	D	PHASE 1	B	S	R	D	PHASE 2	B	S	R	D	PHASE 3
BI & Analytics Platform	Business Intelligence															
	Data Warehouse Mgt		🟦			SQL Server 2012; Visual Studio 11		🟦			SQL Server 2012; Visual Studio 11			🟧		SQL Server 2012; Visual Studio 11
	Big Data															
	Information Services & Marketplaces															
Database & LOB	Transaction Processing															
	Data Management		🟦			Office Professional 2010; SharePoint 2010; SQL Server 2012			🟧		Office Professional 2010; SharePoint 2010; SQL Server 2012			🟧		Office Professional 2010; SharePoint 2010; SQL Server 2012

Platform	Application Infrastructure			🟧		.NET Framework; BizTalk Server 2010; Internet Information Services 8; Office Professional 2010; SharePoint 2010; SQL Server 2012; System Center 2012; Visual Studio 11; Visual Studio 11 Team Foundation Server; Windows Azure AppFabric; Windows Communications Foundation Services; Windows Server 2012; Windows Server AppFabric			🟧		.NET Framework; BizTalk Server 2010; Internet Information Services 8; Office Professional 2010; SharePoint 2010; SQL Server 2012; System Center 2012; Visual Studio 11;Visual Studio 11 Team Foundation Server; Windows Azure AppFabric; Windows Communications Foundation Services; Windows Server 2012; Windows Server AppFabric				🟩	.NET Framework; BizTalk Server 2010; Internet Information Services 8; Office PerformancePoint Server; Office Professional 2010; SharePoint 2010; SQL Server 2012; System Center 2012; Visual Studio 11; Visual Studio 11 Team Foundation Server; Windows Azure; Windows Azure AppFabric; Windows Communications Foundation Services; Windows Server 2012; Windows Server AppFabric
Custom Development	Internet Applications															
	Component & Service Composition															
	Enterprise Integration			🟧		.NET Framework; BizTalk ESB Toolkit; BizTalk Server 2010; SharePoint 2010; SQL Azure; SQL Server 2012; Visual Studio 11			🟧		.NET Framework; BizTalk ESB Toolkit; BizTalk Server 2010; SQL Azure; SQL Server 2012; System Center 2012; System Center 2012 Operations Manager; Visual Studio 11; Windows Azure AppFabric; Windows Server AppFabric			🟧		.NET Framework; BizTalk ESB Toolkit; BizTalk Server 2010; SQL Azure; SQL Server 2012; System Center 2012; System Center 2012 Operations Manager; Visual Studio 11; Windows Azure AppFabric; Windows Server AppFabric
	Development Platform			🟧		Visual Studio 11; Visual Studio 11 Team Foundation Server			🟧		SQL Server 2012; Visual Studio 11; Visual Studio 11 Team Foundation Server; Windows SDK				🟩	SQL Server 2012; Visual Studio 11; Visual Studio 11 Team Foundation Server 2010; Windows SDK
	Application Lifecycle Mgt		🟦			Office Professional 2010; Project 2010; Visual Studio 11; Visual Studio 11 Team Foundation Server			🟧		Office Professional 2010; Project 2010; Visual Studio 11; Visual Studio 11 Team Foundation Server			🟧		Office Professional 2010; Project 2010; Visual Studio 11; Visual Studio 11 Team Foundation Server

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.