Data Center Services

Datacenter Management and Virtualization

1. **What best describes your server and application image maintenance strategy?**

As-is ✔	To-be ✔		
		A.	There is no defined set of core standard images
		B.	A defined set of core standard images exists
		C.	Images are maintained at current update levels and are available for deployment in physical and virtual environments
		D.	Operating system and workload images are maintained in a centralized library to provision new physical and virtual systems on demand for Datacenter services
		E.	Unknown
		F.	Not Applicable
			Comments:

2. **What best describes your application and server workload deployment strategy?**

As-is ✔	To-be ✔		
		A.	Scripted process are used to deploy applications consistently, server provisioning Process is manual and provisioning new server can take weeks.

		B.	There is a defined, end-to-end server deployment process that includes application compatibility testing
		C.	There is an automated, end-to-end server deployment process with task sequencing
		D.	There is an automated, self-service deployment portal where business units can request new IT services for deployment across virtual or private cloud environments. Server provisioning process is automatic and can take minutes.
		E.	Unknown
		F.	Not Applicable
			Comments:

3. **What best describes your patch and update process strategy for data center services?**

As-is ✔	To-be ✔		
		A.	Patch deployment is manual for the majority of servers that run Windows Server
		B.	Deployment and management of software updates are centralized for the majority of servers
		C.	Software update management and auditing are policy-driven and monitored, including automated vulnerability detection
		D.	Isolation and remediation of vulnerable and non-compliant systems are automated. Application and operating system images automatically replaced when issues arise. Live Migration and high availability are used during patching to ensure systems are patched with no downtime.
		E.	Unknown
		F.	Not Applicable

			Comments:

4. What best describes your asset management strategy for servers?

As-is ✔	To-be ✔		
		A.	Hardware and software inventory tracking for servers is manual; no policies, procedures, resources, or tools are in place
		B.	Software asset management processes are automatic and a tool and data repository for hardware and software are in place to track and audit server assets
		C.	The IT software asset life cycle is managed using vision, policies, procedures, and tools; asset and business target management are based on reliable information
		D.	Software mapping spans physical, virtual, and heterogeneous environments and is application-aware with real-time enforcement of compliance for applications that have licensed-based use; all business units follow the same strategy, process, and technology for software asset management
		E.	Unknown
		F.	Not Applicable
			Comments:

5. What best describes your server capacity management and consolidation strategy?

As-is	To-be		

✔	✔		
		A.	There is no capacity planning process for servers
		B.	Capacity management processes for consolidation of business, services, resources, and servers are manual
		C.	Monitoring of current resource needs occurs in real time and utilization is compared to existing capacity; use-analysis tools are used to predict the impact of change (software, hardware, usage, and topology)
		D.	Server provisioning and deprovisioning occur dynamically, on demand, and in real time. Application models and application virtualization allow services to dynamically consume capacity on demand.
		E.	Unknown
		F.	Not Applicable
			Comments:

6. **What best describes your server or service monitoring strategy in data centers?**

As-is ✔	To-be ✔		
		A.	IT system (hardware, hypervisor, OS, and application)-aware monitoring exists for critical servers
		B.	IT system (hardware, hypervisor, OS, and application)-aware monitoring and reporting on the majority of applications are in place across the heterogeneous environment, with defined service-level agreements and manual remediation functionality
		C.	IT system (hardware, hypervisor, OS, and application)-aware monitoring and reporting are in place with basic remediation; there are consolidated views of all management tools and consistent reporting across heterogeneous systems

		D.	IT system (hardware, hypervisor, OS, application and service)-aware monitoring and reporting with full remediation and automated disaster recovery are in place; Service performance and health monitoring drives advanced management of how datacenter resources are used
		E.	Unknown
		F.	Not Applicable
		Comments:	

7. **What best describes your organization's server virtualization and Private Cloud progress?**

As-is ✔	To-be ✔		
		A.	Virtualized layers are not offered as a service within the company.(No Private Cloud)
		B.	Some Production server resources are virtualized.A virtualized server pool is being offered as services (minimal Private Cloud progress).
		C.	Majority of production server resources are virtualized.A virtualized server pool is offered as a service (Private Cloud Exists).Several Compliance and cost savings strategies leverage that Private Cloud. (Auditing and Reporting, Policy Management, Metering Usage, Process Automation etc...)
		D.	Majority of production server resources are virtualized. A virtualized server pool is offered as a service (Private Cloud Exists). Several Quality (Process Excellence, Business Continuity etc..) and agility (Real time elasticity, self service automation etc...) strategies leverage that Private Cloud. Integrated management across phsical, Virtual and Workloads.
		E.	Unknown
		F.	Not Applicable

As-is ✔	To-be ✔		
			Comments:

8. **What best describes your server compliance policy?**

As-is ✔	To-be ✔		
		A.	A documented policy is in place for configuration and compliance of servers and IT systems
		B.	Servers and IT systems are audited for compliance based on documented company and industry-standard policies (HIPPA, SOX, and PCI); reports are generated monthly
		C.	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 data center services
		D.	Real-time policy enforcement and reporting are based on company and industry-standard polices with automated non-compliance resolution for all data center services
		E.	Unknown
		F.	Not Applicable
			Comments:

9. **What best describes your high-availability strategy?**

As-is ✔	To-be ✔		

		A.	There is no high-availability strategy
		B.	Services are available during server failure (via server clustering or hot spares)
		C.	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
		D.	Services are available during complete site outage (via geo-clustering and automated management)
		E.	Unknown
		F.	Not Applicable
			Comments:

10. What best describes your server virtualization strategy?

As-is ✔	To-be ✔		
		A.	No server virtualization or server virtualization used only in test environments
		B.	The organization actively uses virtualization to consolidate servers for production workloads
		C.	The organization has a consolidated view of and a consolidated management process for heterogeneous virtual environments, including branch offices
		D.	The organization uses virtualization to manage resource allocation dynamically for workloads and services including moving workloads from server to server based on resource needs or business rules
		E.	Unknown
		F.	Not Applicable

			Comments:

11. What Best Describes your IT Service Charge Back Process?

As-is ✔	To-be ✔		
		A.	No Charge back process
		B.	Limited process in place to assign costs for IT Services back to business groups
		C.	Per-project charge back based on hardware and software acquisition cost and based on resources allocated to the project.
		D.	Real-time monitoring of IT systems with charge back engines to business groups consuming IT Services
		E.	Unknown
		F.	Not Applicable
			Comments:

12. What Best Describes your Hypervisor/Virtualization protection? (Multi Tenancy)

As-is ✔	To-be ✔		
		A.	No Segmentation for services provided on virtualization hosts. Isolation happen of the physical infrastructure.

		B.	Users can only have visibility into specific VM's based on business units but manual security isolation exists between the VM's themselves.
		C.	Security isolation exists between VM's with some automation of the isolation rules.
		D.	Full Isolation of VM's based on Hierarchical view of the organization. Isolation rules kept when moving VM between physical hosts.
		E.	Unknown
		F.	Not Applicable
			Comments:

Data Center Services

Server Security

13. What best describes your server operating system protection strategy?

As-is ✔	To-be ✔		
		A.	There is no malware protection, or unmanaged malware protection exists for some server operating systems
		B.	Malware protection is centrally managed across server operating systems, including the host firewall
		C.	Malware protection is centrally managed across server operating systems, including host firewall, host IPS/vulnerability shielding, and quarantine
		D.	Malware protection is centrally managed and comprehensive for server operating systems, and includes automated remediation, recovery, and auditing
		E.	Unknown
		F.	Not Applicable

			Comments:

14. What best describes your application protection strategy for servers?

As-is ✔	To-be ✔		
		A.	Applications are not protected, or protection is unmanaged
		B.	Protection for select applications (such as e-mail) is centrally managed
		C.	Protection for all collaboration applications (such as e-mail, document sharing, and instant messaging) is centrally managed
		D.	Protection is comprehensive, specifically deployed and managed on multiple tiers for all applications in the enterprise, including proprietary applications
		E.	Unknown
		F.	Not Applicable
			Comments:

15. What best describes your network protection strategy?

As-is ✔	To-be ✔		
		A.	There is no network security, or network security is limited to basic perimeter firewall

		B.	Multiple vendor products are used for firewall, IPS, Web security, gateway anti-virus, and URL filtering
		C.	Integrated perimeter firewall, IPS, Web security, gateway anti-virus, and URL filtering are deployed with support for server and domain isolation
		D.	Network security is automated and proactive, with centralized alerting and reporting to meet network protection service-level agreements; network security, alerts, and compliance are integrated with all other company tools to provide a complete and company-wide scorecard view and threat assessment that includes private and public cloud environments
		E.	Unknown
		F.	Not Applicable
			Comments:

16. What best describes your secure remote access strategy?

As-is ✔	To-be ✔		
		A.	Remote client access is limited or non-existent
		B.	Remote access is secure, standardized, and available to end users across the organization
		C.	Secure remote access is integrated with quarantine for compliance with corporate policy
		D.	Secure, remote access is nearly always available with bidirectional connectivity; access to networks and applications is policy-based; alerts are proactive and security issues are remediated
		E.	Unknown
		F.	Not Applicable

			Comments:

Data Center Services

Networking

17. What best describes your Domain Name System management strategy?

As-is ✔	To-be ✔		
		A.	Zones and records are created manually
		B.	Zone creation and record updates are automatic to support directory services
		C.	Automatic server cleanup uses scavenging
		D.	User auditing and reporting is based on zones
		E.	Unknown
		F.	Not Applicable
			Comments:

18. What best describes your Domain Name System resilience strategy?

As-is ✔	To-be ✔		
		A.	The Domain Name System server is a single server
		B.	Redundant Domain Name System servers exist in a single location and

			provide fault tolerance
		C.	Redundant Domain Name System servers exist in multiple locations and provide fault tolerance
		D.	The Domain Name System is self-healing
		E.	Unknown
		F.	Not Applicable
			Comments:

19. What best describes your Dynamic Host Configuration Protocol management strategy?

As-is ✔	To-be ✔		
		A.	A Dynamic Host Configuration Protocol server is deployed and configured for IPv4 settings with options related to network connectivity (such as subnet mask and gateway)
		B.	A Dynamic Host Configuration Protocol server dynamically registers the client host name IP address; the Domain Name System presents a unified view to the namespace
		C.	A Dynamic Host Configuration Protocol server is deployed and configured for IPv6 settings with options related to network connectivity (such as subnet mask and gateway)
		D.	Dynamic Host Configuration Protocol servers are integrated with Network Access Policy for network access control and security
		E.	Unknown
		F.	Not Applicable
			Comments:

20. What best describes your Dynamic Host Configuration Protocol infrastructure strategy?

As-is ✓	To-be ✓		
		A.	Dynamic Host Configuration Protocol servers are not network-aware
		B.	Dynamic Host Configuration Protocol servers are aware of sub-networks
		C.	The Dynamic Host Configuration Protocol infrastructure is aware of the virtual local area network
		D.	The Dynamic Host Configuration Protocol infrastructure is client-aware (for example, VoIP clients, desktop systems, and similar)
		E.	Unknown
		F.	Not Applicable
			Comments:

21. What best describes your network quality of service strategy?

As-is ✓	To-be ✓		
		A.	There is simple monitoring of network device outages
		B.	Network quality of service (basic prioritization of applications and services) is standard, with manual allocation of available bandwidth
		C.	Quality of service is in place for prioritizing applications and services with

			intelligent allocation of bandwidth. Network capacity is virtualized and available via pools that are consumed by VMs and services based on dynamic management driven by service models.
		D.	Allocation of bandwidth is on-demand and automatically scales to meet additional network requirements based on data center service requirements. Network resources are pooled and made available on demand to services and VMs based on policies and models that drive management of these resources
		E.	Unknown
		F.	Not Applicable
			Comments:

22. What best describes your network branch optimization strategy?

As-is ✔	To-be ✔		
		A.	There is no caching technology
		B.	The deployment model for files and intranet traffic uses distributed caching
		C.	The deployment model and configuration of the hosted cache is centralized and based on policy (Main workloads include application streaming, software deployment, patches, and updates)
		D.	There is full, end-to-end integration of network optimization solutions with heterogeneous network traffic
		E.	Unknown
		F.	Not Applicable
			Comments:

23. What best describes your wide area network monitoring strategy?

As-is ✔	To-be ✔		
		A.	Wide area network health and performance are not monitored or reported
		B.	Branch traffic health and performance are monitored and reported manually
		C.	Branch traffic health and performance is monitored and reported centrally, supported by management tools
		D.	Cache systems and data are centralized, pre-populated, fully managed, and integrated with the networking management infrastructure
		E.	Unknown
		F.	Not Applicable
			Comments:

Data Center Services

Storage

24. What best describes your storage management strategy?

As-is ✔	To-be ✔		
		A.	Storage is managed on physical disks

		B.	Storage is managed on individual servers or disk arrays
		C.	Storage is managed on server clusters or shared storage arrays
		D.	Storage is managed in highly available storage pools that are consumed by VMs and services based on dynamic management driven by service models
		E.	Unknown
		F.	Not Applicable
			Comments:

25. What best describes your storage availability strategy?

As-is ✔	To-be ✔		
		A.	Users are notified about data integrity errors, but data loss is possible if a disk or system component fails
		B.	No data is lost if a single disk or system component fails, but data availability may be interrupted
		C.	Transparent failover occurs if a storage node fails, with no interruption in availability
		D.	Critical data can be replicated between geographical or virtual locations or services to help ensure business continuity in the event of a site failure
		E.	Unknown
		F.	Not Applicable
			Comments:

26. What best describes your storage access strategy?

As-is ✔	To-be ✔		
		A.	Users access their own files from local disks, and shared data from servers
		B.	Users access files and frequently used information from caches on local disks or servers in local offices, even if primary servers are remote; users can access personal files stored on a server from other PCs
		C.	Actively used data is geographically distributed or replicated to multiple servers; users have seamless access to most available servers by using a single namespace
		D.	Mobile users have secure access to actively used data whether or not they are connected to the enterprise network; they also can access data securely from Internet kiosks
		E.	Unknown
		F.	Not Applicable
			Comments:

27. What best describes your storage discovery strategy?

As-is ✔	To-be ✔		
		A.	No comprehensive map of all stored data exists, nor does a predefined plan for identifying and retrieving electronically stored information; data is indexed only on computers where it is stored
		B.	A defined e-discovery policy and manual processes exist for identifying and retrieving electronically stored information

		C.	An automated process for identifying and retrieving electronically stored information exists; auditing and reporting on compliance with an e-discovery policy is supported
		D.	Storage system indexing is integrated with business intelligence for aggregation of stored data for trend analysis and planning
		E.	Unknown
		F.	Not Applicable
			Comments:

28. What best describes your sensitive information storage strategy?

As-is ✔	To-be ✔		
		A.	Sensitive information is stored with other data, and access is protected by user names and passwords
		B.	Sensitive information is stored in disconnected systems or is manually placed in password-protected locations to prevent unauthorized access
		C.	Automatic processes enable identification of sensitive information based on business policy, and to store sensitive information in appropriate locations
		D.	Sensitive information is identified and encrypted automatically when it is used or stored, based on business policy use, so sensitive information is prevented from leaving enterprise control
		E.	Unknown
		F.	Not Applicable
			Comments:

29. What best describes your data classification strategy?

As-is ✔	To-be ✔		
		A.	Data is not classified, or only as organized by individual users
		B.	Data is classified manually or based on location in a folder hierarchy
		C.	Archiving, deletion, and life cycle processes occur based on data classification; data classification is also used to enforce corporate security policies and to control data access mechanisms (such as per session, virtual desktop infrastructure, and remote procedure calls)
		D.	Data is classified automatically based on properties and file content; archiving, deletion, and life-cycle processes occur based on data classification
		E.	Unknown
		F.	Not Applicable
			Comments:

30. What best describes your storage allocation strategy?

As-is ✔	To-be ✔		
		A.	Storage is allocated locally on physical disk volumes based on capacity
		B.	Storage is allocated in file shares or logically on shared, fixed-size disk volumes
		C.	Storage is allocated in file shares on highly available servers, on virtual disks, or dynamically on disk volumes

As-is	To-be		
		D.	Storage is allocated dynamically from an available pool of physical space based on capacity required, and within limits set by policy quotas
		E.	Unknown
		F.	Not Applicable
			Comments:

31. What best describes your backup and recovery strategy for servers?

As-is ✔	To-be ✔		
		A.	Critical data is backed up and restored manually, in multiple locations where the data is stored
		B.	Critical data is backed up on a schedule across the enterprise; backup copies are stored offsite
		C.	Critical data is backed up by taking snapshots using a centralized, application-aware system; backup copies are stored separately at a physical location or by using a cloud-based service, with fully tested recovery or failover based on service-level agreements
		D.	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
		E.	Unknown
		F.	Not Applicable
			Comments:

32. What best describes your data archiving strategy?

As-is ✔	To-be ✔		
		A.	Data is archived manually
		B.	Data is archived automatically based on storage quotas and date of last modification or access
		C.	Data is managed based on storage location by using automated compliance and retention policies such as rights management, read-only storage, and file expiration
		D.	Data is managed and archived automatically based on policy across multiple servers in the enterprise; management and auditing are centralized
		E.	Unknown
		F.	Not Applicable
			Comments:

33. What best describes your data de-duplication strategy?

As-is ✔	To-be ✔		
		A.	Multiple copies of duplicate files are stored separately
		B.	Data de-duplication occurs at the file level on individual servers or storage devices
		C.	Data de-duplication occurs at the block or sub-file level on individual servers or storage devices
		D.	Data de-duplication and compression occurs at the sub-file level across all servers and storage devices, and is integrated with file access to

			optimize network transfers
		E.	Unknown
		F.	Not Applicable
			Comments:

Client Services

Client Management and Virtualization

34. What best describes your client image management and deployment strategy?

As-is ✔	To-be ✔		
		A.	Standard images may be present for desktop deployment; deployment is manual
		B.	An image library and deployment process are in place for operating systems
		C.	The operating system image deployment process is automated, zero-touch, and layered for desktop systems (physical or virtual)
		D.	Deployment tools deliver appropriate operating system and application services based on user needs and the capabilities of connecting devices
		E.	Unknown
		F.	Not Applicable
			Comments:

35. What best describes your operating system policy strategy for clients?

As-is ✔	To-be ✔		
		A.	There is no consistent operating system deployment strategy
		B.	The majority of the installed client base has a minimum of one year of mainstream support remaining
		C.	The majority of the installed client base has a combination of current and recently released operating systems
		D.	The majority of the installed client base has the current operating system version deployed within eighteen months of initial release
		E.	Unknown
		F.	Not Applicable
d			**Comments:**

36. What best describes your roaming user profiles strategy across the organization?

As-is ✔	To-be ✔		
		A.	Individual users have multiple, unintegrated profiles
		B.	A centralized store of user profiles enables profiles to roam with users
		C.	A centralized store of user profiles supports the ability to apply policies
		D.	A centralized store of user profiles and policies enables user control and automated synchronization across applications and devices
		E.	Unknown
		F.	Not Applicable

			Comments:

37. What best describes your client backup and recovery strategy?

As-is ✔	To-be ✔		
		A.	Data backup is manual, so the user state is dependent on an individual machine
		B.	Users back up critical data locally according to corporate policy and by using the tool provided; when it is necessary, user state can be abstracted from the operating system image (such as for a session, virtual desktop infrastructure, or roaming profile)
		C.	Storage of user state is centralized, including retention policies that align with corporate mandates (security and policy)
		D.	Backup of client data is centralized and supports self-service recovery capabilities to restore the user state to newly provisioned images—almost instantaneously
		E.	Unknown
		F.	Not Applicable
			Comments:

38. What best describes your application deployment and control strategy for clients?

As-is ✔	To-be ✔		

		A.	The majority of applications is deployed manually with limited policies
		B.	Software distribution to local and geographically dispersed users is automated
		C.	Software is available to users based on user identity rather than device; software "follows" users as they move from one device to another
		D.	Users have self-service capabilities to find, request, and install approved applications appropriate to their jobs
		E.	Unknown
		F.	Not Applicable
			Comments:

39. What best describes your application virtualization strategy?

As-is ✔	To-be ✔		
		A.	There is no use of application virtualization
		B.	Some applications are virtualized, but most are installed as packages or are included in the standard image
		C.	Applications are distributed on demand for the majority of traditional desktop environments and productivity applications
		D.	Applications are distributed on demand for the majority of traditional desktop environments, and desktop services are delivered through a virtual desktop infrastructure or virtual session architecture for the majority of productivity applications
		E.	Unknown
		F.	Not Applicable

			Comments:

40. What best describes your application compatibility strategy?

As-is ✔	To-be ✔		
		A.	There is no application compatibility testing solution
		B.	An application compatibility testing solution is in place to assist in identifying and managing the overall application portfolio
		C.	Application compatibility testing is documented and standardized; incompatibilities are mitigated by re-coding or applying fixes (shims)
		D.	Application compatibility testing is managed by an automated test suite; user interaction is minimal and incompatibilities are remediated automatically
		E.	Unknown
		F.	Not Applicable
			Comments:

41. What best describes your patch management strategy for desktop systems?

As-is ✔	To-be ✔		
		A.	There is no centralized patch management for desktop systems

		B.	System and security updates are distributed and installed automatically for desktop systems
		C.	A unified solution offers a single view to manage security patches and to detect current and emerging malware, viruses, and other threats automatically; non-compliant systems are remediated automatically
		D.	Users are granted network access only after passing automatic inspection of connecting devices; non-compliant systems are remediated automatically
		E.	Unknown
		F.	Not Applicable
			Comments:

42. What best describes your desktop monitoring strategy?

As-is ✔	To-be ✔		
		A.	Desktop systems and system events are not centrally monitored
		B.	Desktop applications and system events are centrally monitored for critical desktop systems
		C.	Desktop applications and system events are centrally monitored and reported, and trends are analyzed and integrated into incident management systems
		D.	Desktop applications and system events are centrally monitored in real time according to service-level agreements; heuristic scanning is in place and remediation is automatic
		E.	Unknown
		F.	Not Applicable

			Comments:

43. What best describes your configuration compliance strategy for clients?

As-is ✔	To-be ✔		
		A.	There are no standardized baseline configurations for client systems
		B.	Configurations are standardized; systems are assessed for compliance, and some settings are enforced through group policies
		C.	Configuration is enforced according to a system based on company and industry-standard polices; an authoritative configuration management database is kept up to date
		D.	Configuration is enforced in real time according to centralized company and industry-standard policies; non-compliance is automatically resolved
		E.	Unknown
		F.	Not Applicable
			Comments:

44. What best describes your asset management strategy for clients?

As-is ✔	To-be ✔		
		A.	There is little control over which IT assets are being used and where; the organization lacks policies, procedures, resources, and tools
		B.	Hardware and software inventory is automated and reporting is

			centralized; information may not be complete or accurate, and typically is not used for decision-making; inventory is reconciled annually
		C.	Software installed in physical and virtual environments is identified and categorized automatically; there is a single location to track license and contract details and to manage the software allocation; inventory is reconciled quarterly
		D.	Tracking processes for IT asset policies are automated; comprehensive reporting covers procurement to decommissioning, based on a single inventory or configuration management database; overall business objectives include strategic asset management. Inventory is reconciled continually
		E.	Unknown
		F.	Not Applicable
			Comments:

45. What best describes your mobile device provisioning strategy?

As-is ✔	To-be ✔		
		A.	Mobile devices are configured and synchronized with desktop systems manually
		B.	Mobile service configuration is automated and occurs over-the-air
		C.	Certificate provisioning and authorization (for example, 802.1x or Secure Sockets Layer) is in place for mobile devices
		D.	Non-compliant mobile devices are remediated automatically
		E.	Unknown
		F.	Not Applicable

			Comments:

46. What best describes your device management strategy?

As-is ✔	To-be ✔		
		A.	Devices are managed manually
		B.	A solution is in place to configure and update devices.
		C.	A solution is in place to automatically identify devices to deploy, configure and update while maintaining device security.
		D.	There is an automated solution for federated management of all devices.
		E.	Unknown
		F.	Not Applicable
			Comments:

47. What best describes your mobile usage strategy for line-of-business applications?

As-is ✔	To-be ✔		
		A.	Mobile phones are used for voice communications only
		B.	Mobile phones are used for over-the-air synchronization with e-mail, calendar, and contacts
		C.	Mobile devices are used to access lightweight line-of-business applications

		D.	Mobile devices have full access to line-of-business applications
		E.	Unknown
		F.	Not Applicable
			Comments:

48. What best describes your security policy strategy for mobile devices?

As-is ✔	To-be ✔		
		A.	Mobile devices are managed by security policy provisioning (such as personal identification numbers) and remote deletion
		B.	Mobile devices are managed by enforceable application and hardware policies (such as device encryption and hardware access)
		C.	Mobile devices are managed and integrated with core infrastructure services for policy configuration and enforcement including multi-factor authentication
		D.	None
		E.	Unknown
		F.	Not Applicable
			Comments:

49. What best describes your mobile software management strategy?

As-is	To-be		

✔	✔		
		A.	There is no software distribution for mobile devices
		B.	Installation and inventory of standard corporate applications on mobile devices are manual
		C.	Installation and inventory of standard corporate applications on mobile devices are managed automatically through integrated software distribution tools
		D.	Mobile devices are managed across multiple platforms to allow end users to self-provision applications, control settings, and manage device updates intelligently
		E.	Unknown
		F.	Not Applicable
			Comments:

Client Services

Client Security

50. What best describes your mobile remote access strategy?

As-is ✔	To-be ✔		
		A.	All mobile access to internal systems is proxied through the messaging system
		B.	Mobile access to internal systems is granted through a virtual private network (IP Security or SSL)
		C.	Mobile devices can initiate direct access to internal corporate resources
		D.	None

As-is	To-be		
		E.	Unknown
		F.	Not Applicable
			Comments:

51. What best describes your strategy for protecting clients against malware?

As-is ✔	To-be ✔		
		A.	Protection against malware is unmanaged or non-existent for desktop systems and laptops
		B.	Protection against malware is centrally managed for desktop systems and laptops and includes a host firewall; non-PC devices are managed and protected through a separate process
		C.	Protection against malware is centrally managed for desktop systems, laptops, and non-PC devices; desktop systems and laptops include a host firewall, host intrusion prevention system or vulnerability shield, and quarantine
		D.	Protection against malware is comprehensive and centrally managed for desktop systems, laptops, and non-PC devices; remediation, recovery, and auditing are automated
		E.	Unknown
		F.	Not Applicable
			Comments:

52. What best describes your client lockdown strategy?

As-is ✔	To-be ✔		
		A.	End users are local administrators throughout the desktop environment
		B.	All users are deployed as standard users by default, and administrative access is given as needed
		C.	All users are deployed as standard users, and users who require administrative access are given secondary accounts; users are restricted from running applications that are considered harmful to the environment
		D.	Application control technologies are used to determine exactly what runs in the enterprise desktop environment
		E.	Unknown
		F.	Not Applicable
			Comments:

53. What best describes your client encryption strategy?

As-is ✔	To-be ✔		
		A.	There is no client-side encryption of disks, files, or folders
		B.	Disk-level encryption is in place for select laptops and devices that have a high business impact
		C.	Disk-level encryption is in place across all desktop systems and laptops; file and folder encryption are manual or semi-automated
		D.	Disk, file, and folder encryption are automatically applied across all desktop systems, laptops, and peripheral storage devices based on centrally administered policy

		E.	Unknown
		F.	Not Applicable
			Comments:

Identity and Security Services

Identity and Access

54. What best describes your identity provisioning and access management strategy?

As-is ✔	To-be ✔		
		A.	User account provisioning and de-provisioning are manual and access is controlled per instance
		B.	Limited, simple provisioning and de-provisioning of user accounts, mailboxes, certificates, smart cards, and machines exists to control access
		C.	Provisioning and de-provisioning of user and super-user accounts, certificates, and smart cards is automated; access control is role-based
		D.	Provisioning and de-provisioning of all resources, certificates, and smart cards is automated for all users; roles and entitlement are managed and access control is policy-driven
		E.	Unknown
		F.	Not Applicable
			Comments:

55. What best describes your password and group management strategy?

As-is ✔	To-be ✔		
		A.	There is no end-user self-service for password resets and group management
		B.	Password resets and group management are limited, through custom in-house tools or manual processes
		C.	Self-service password resets, group management, and related capabilities are supported by workflows
		D.	Rich capabilities are in place for self-service access management, including dynamic group management, across IT and line-of-business applications
		E.	Unknown
		F.	Not Applicable
			Comments:

56. What best describes your identity federation strategy?

As-is ✔	To-be ✔		
		A.	There is no federation of identity
		B.	Federation and trust are set manually per instance for select applications or systems across boundaries
		C.	The federation and trust management infrastructure is standardized for applications and systems that cross boundaries
		D.	The federation and trust management infrastructure is fully automated for partner and cloud-based scenarios to readily enable user-based

			access
		E.	Unknown
		F.	Not Applicable
			Comments:

57. What best describes your authentication strategy?

As-is ✔	To-be ✔		
		A.	Authentication is based on simple passwords with no IT policies
		B.	Password policies are set within the directory service to enable life-cycle management
		C.	Multi-factor and certificate-based authentication are applied in high-risk scenarios, such as remote access or document signing
		D.	Multi-factor and certificate-based authentication are corporate-wide across all applications and users
		E.	Unknown
		F.	Not Applicable
			Comments:

58. What best describes your authorization strategy?

As-is ✔	To-be ✔		

		A.	Authorization is based on manual processes
		B.	There is a centralized access policy for business resources, with some standardization in the policy
		C.	A centralized, common-access policy is defined for business resources, applications, and information resources; entitlement is managed
		D.	End-users can have multiple identities to enable seamless, dynamic role changes (for example, consumer to information worker) based on contextual access enforced by corporate policy
		E.	Unknown
		F.	Not Applicable
			Comments:

59. What best describes your application directory service strategy?

As-is ✔	To-be ✔		
		A.	There is no application directory service
		B.	Multiple application directory services exist to support multiple standards
		C.	A single application directory service covers multiple standards and most applications
		D.	A single application directory service covers multiple standards and all applications in the corporate directory
		E.	Unknown
		F.	Not Applicable
			Comments:

60. What best describes your directory services strategy?

As-is ✔	To-be ✔		
		A.	Multiple, isolated directories use varied authentication methods
		B.	Most applications and services share a common directory for authentication; some point-to-point synchronization exists across different directories, applications, and repositories
		C.	A centralized, scalable directory works across geographies for all intranet applications, and supports authentication and authorization
		D.	A centralized directory supports all intranet, extranet, and Internet scenarios, and automatically synchronizes with all remaining directories
		E.	Unknown
		F.	Not Applicable
			Comments:

Identity and Security Services

Information Protection & Control

61. What best describes your strategy for protecting data at rest?

As-is ✔	To-be ✔		

		A.	Discovery, classification, and protection of data stored on servers or in the back office is non-existent
		B.	Data discovery and protection is supported by technologies and processes for some servers and back-office endpoints; individual users drive data classification
		C.	Data discovery and protection is supported for desktop endpoints in addition to servers and back-office endpoints; data classification is driven by context and end users
		D.	Data discovery, protection, and classification (contextual and policy-driven) are implemented across the enterprise
		E.	Unknown
		F.	Not Applicable
			Comments:

62. What best describes your strategy for protecting data in motion?

As-is ✔	To-be ✔		
		A.	Discovery, classification, and protection are random for data that is transmitted through the network via e-mail and other means
		B.	There are technologies and processes for discovery, user-driven classification, and protection of data at select points and for select protocols in the network (for example, at gateways or in e-mail)
		C.	Data classification is contextual at select points and for select protocols in the network, and complements classification by end users
		D.	There is end-to-end discovery, classification (contextual and policy-driven), and protection across all waypoints and supporting all protocols within the enterprise
		E.	Unknown

		F.	Not Applicable
			Comments:

63. What best describes your strategy for protecting data in use?

As-is ✔	To-be ✔		
		A.	Discovery, classification, and protection are random for data that is created and used at endpoints such as desktop systems and laptops
		B.	There are technologies and processes for discovery and protection of data that is created and used at select endpoints; individual users drive data classification
		C.	Data classification is both contextual and driven by end-users as data is created and used
		D.	There is end-to-end discovery, classification (contextual and policy-driven), and protection across all endpoints as data is created and used
		E.	Unknown
		F.	Not Applicable
			Comments:

64. What best describes your information protection policy?

As-is ✔	To-be ✔		

		A.	Basic information protection is in place with simple policies to restrict use (such as drive and folder encryption)
		B.	Persistent information protection exists within the trusted network to enforce policy across key sensitive data (such as documents and e-mail)
		C.	Persistent information protection helps to enforce policy on sensitive data across the enterprise, including data on mobile devices; policy templates are used to standardize rights and control access to information
		D.	Persistent information protection is automated for sensitive data across the partner and customer ecosystem
		E.	Unknown
		F.	Not Applicable
			Comments:

65. What best describes your strategy for information protection reporting?

As-is ✔	To-be ✔		
		A.	Auditing and reporting are manual processes
		B.	Reporting is predefined for select server and back-office waypoints
		C.	Reporting is customized for server, back-office, and end-user waypoints; there is limited capability to investigate some incidents
		D.	Reporting is rich and automated; incident tracking enables root-cause analysis and remediation
		E.	Unknown
		F.	Not Applicable
			Comments:

IT Process and Compliance

IT Process and Compliance

66. What best describes your strategy to plan for alignment of IT services?

As-is ✔	To-be ✔		
		A.	Business strategy and IT strategy occasionally are aligned; measurement of IT service capacity, availability, continuity, and data integrity is unmanaged; IT service costs and returns are sometimes recognized
		B.	Individual business units align with the IT service portfolio; IT service costs, returns, capacity, availability, continuity, and integrity are reported
		C.	The organization aligns with the IT service portfolio; management regularly reviews how the service portfolio and strategy align, and reports costs and returns across IT services
		D.	All IT services are described in the service portfolio; services align with business strategy; IT service costs and returns can be modeled and predicted
		E.	Unknown
		F.	Not Applicable
			Comments:

67. What best describes your strategy to plan for IT service policies?

As-is ✔	To-be ✔		

		A.	IT policies are developed and stored occasionally
		B.	IT policies are documented for each IT service
		C.	IT policies are integrated across all IT services
		D.	IT policies initiate automated remediation
		E.	Unknown
		F.	Not Applicable
			Comments:

68. What best describes your strategy to plan for IT service reliability?

As-is ✔	To-be ✔		
		A.	IT service reliability is defined occasionally
		B.	Each IT service has a formal definition of reliability
		C.	Definitions of reliability for IT services are integrated across IT services
		D.	Definitions of reliability for IT services are modeled
		E.	Unknown
		F.	Not Applicable
			Comments:

69. What best describes your project planning strategy for IT services?

As-is ✔	To-be ✔		
		A.	IT service project plans and functional specifications are developed occasionally
		B.	IT service projects are started with a clear vision, scope, and team, and appropriate specifications are in place
		C.	IT service projects are aligned with business projects through participation of customers; each project has a management review for project plan approval
		D.	IT service project management is integrated with change management, service catalogue definitions and modeling.
		E.	Unknown
		F.	Not Applicable
			Comments:

70. **What best describes your strategy for building and stabilizing the delivery of IT services and testing procedures?**

As-is ✔	To-be ✔		
		A.	Bug handling, design changes, and testing are not formally managed for IT services
		B.	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
		C.	IT service issues and design changes are tracked by using formal processes; testing is automated where possible

		D.	IT service testing is automated
		E.	Unknown
		F.	Not Applicable
			Comments:

71. What best describes your strategy for IT services deployment?

As-is ✔	To-be ✔		
		A.	IT service release and deployment processes are not formally managed
		B.	IT service release and deployment processes are standardized
		C.	IT service release processes are uniform across IT services; deployment is automated where possible; management reviews each service for readiness to release before deployment
		D.	IT service deployment is fully automated and driven by self service access by business users.
		E.	Unknown
		F.	Not Applicable
			Comments:

72. What best describes your strategy for IT service operations and service-level agreements?

As-is	To-be		

✔	✔		
		A.	Service-level or operational-level agreements are not formally managed
		B.	Each IT service provides service-level or operational-level agreements
		C.	Service-level and operational-level agreements are integrated across IT services; management reviews operational health regularly; some tasks are automated
		D.	Reporting on service-level and operational-level agreements occurs in real time across the organization; IT services are provisioned dynamically to provide the required levels of reliability and scalability; all tasks that can be automated are automated
		E.	Unknown
		F.	Not Applicable
			Comments:

73. What best describes your strategy for IT service incident management?

As-is ✔	To-be ✔		
		A.	IT service incidents are not formally managed
		B.	Processes to manage incidents and problems are in place for each IT service
		C.	Processes to manage incidents are integrated across IT services
		D.	Standard changes to IT services are managed by self-service provisioning where appropriate
		E.	Unknown
		F.	Not Applicable

			Comments:

74. What best describes your service monitoring strategy for IT services?

As-is ✔	To-be ✔		
		A.	Monitoring, reporting, and auditing tools are not formally managed for IT services
		B.	Monitoring, reporting, and auditing are in place for IT services
		C.	Monitoring, reporting, and auditing are integrated across IT services; some capabilities exist for event investigation, analysis, and forensics
		D.	Monitoring, reporting, and auditing are automated across IT services—including dynamic correlation to identify patterns, respond proactively to issues, and coordinate across teams
		E.	Unknown
		F.	Not Applicable
			Comments:

75. What best describes your strategy for monitoring security and reporting on IT services?

As-is ✔	To-be ✔		
		A.	Monitoring and reporting are not formally managed for protection

			against malware, protection of information, and identity and access technologies
		B.	Monitoring and reporting are centralized for protection against malware, protection of information, and identity and access technologies
		C.	Monitoring and reporting are integrated with individual areas for protection against malware, protection of information, and identity and access technologies
		D.	Monitoring, reporting, and auditing are automated with event correlation and remediation for protection against malware, protection of information, and identity and access technologies
		E.	Unknown
		F.	Not Applicable
			Comments:

76. What best describes your problem management strategy for IT services?

As-is ✔	To-be ✔		
		A.	IT service problems are not formally managed
		B.	Incident and problem management processes are in place for each IT service
		C.	Problem management processes are integrated across IT services
		D.	IT services are analyzed automatically for potential problems; preventative actions are automated
		E.	Unknown
		F.	Not Applicable

As-is	To-be		
			Comments:

77. What best describes your change and configuration management strategy for IT services?

As-is ✔	To-be ✔		
		A.	The IT service change and configuration process is not formally managed
		B.	Each IT service has its own change and configuration management process; standard changes are identified for each IT service
		C.	The change and configuration management process is integrated across IT services; standard changes are identified across IT services and automated where possible
		D.	All standard changes across IT services are automated and provisioned by self-service processes where appropriate
		E.	Unknown
		F.	Not Applicable
			Comments:

78. What best describes your IT services team accountability and management strategy?

As-is ✔	To-be ✔		
		A.	IT service owners and accountability are not formally assigned

		B.	Ownership and accountability are assigned for each IT service
		C.	Ownership and accountability assignments are integrated across all IT services
		D.	The organization can quickly adapt to changing business needs
		E.	Unknown
		F.	Not Applicable
			Comments:

79. What best describes your IT compliance strategy for IT services?

As-is ✔	To-be ✔		
		A.	Risk and vulnerability analysis of IT service confidentiality, integrity, and availability is not formally managed; IT compliance objectives and activities are not defined
		B.	Risk and vulnerability are formally analyzed for each IT service; IT compliance objectives and activities are defined for each IT service
		C.	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 reviews policy and compliance
		D.	Risks and vulnerabilities are analyzed across all IT services against developed models; compliance objectives and activities are automated, and then updated automatically based on changes to IT policies
		E.	Unknown
		F.	Not Applicable
			Comments:

Collaboration

Workspaces

80. What best describes your provisioning and architecture for collaborative workspaces?

As-is ✔	To-be ✔		
		A.	Individual workspaces are created by using products from multiple vendors and are not managed, nor are they integrated with productivity tools
		B.	Workspaces are managed at the departmental level and are available from individual productivity applications
		C.	Workspaces are centrally managed, customizable, and reusable, and provide users the capability to collaborate through Web browsers and mobile devices; offline synchronization is supported
		D.	Workspaces are centrally managed, support a hybrid on-premises and Web (cloud)-based infrastructure, and integrate fully with business applications; life-cycle management, including creation, discoverability, archiving, and retirement, is automated
		E.	Unknown
		F.	Not Applicable
			Comments:

81. What best describes your experience of team collaboration?

As-is ✔	To-be ✔		
		A.	Team collaboration occurs through e-mail without any provision of common management and storage
		B.	Teams work on managed versions of content with controls and common space; team workspaces include group calendaring, shared contacts, user online presence, and simple workflows
		C.	Team members can simultaneously author, edit, and review content across Clients (including Devices)
		D.	Team collaboration is integrated with line-of-business applications for content creation
		E.	Unknown
		F.	Not Applicable
			Comments:

Collaboration

Portals

82. What best describes your content publishing strategy?

As-is ✔	To-be ✔		
		A.	Content is static and is not targeted or personalized; specialists and special tools are required to publish most content
		B.	Users and groups can publish content directly to some portals; workflow for review and approval is built-in and automated
		C.	Publishers can direct content to specific audience targets; portals deliver a

			customized, targeted, or aggregated view of information to individuals based on user identity, role & device on which content is consumed.
		D.	Users can publish content to extranet and Internet sites with the same systems, device form-factors and methods they use to publish content to the intranet; in addition, users can publish content that includes line-of-business data to portals from within business and productivity applications
		E.	Unknown
		F.	Not Applicable
			Comments:

83. What best describes your user experience for portals?

As-is ✔	To-be ✔		
		A.	Users are passive readers of content; there is no single sign-on capability or effective enterprise search across portals
		B.	Users have widgets to customize their views of information; enterprise search is integrated with portals
		C.	Users get targeted information based on their profiles , their roles in the organization & mobile devices being used
		D.	Users have rich, targeted, meaningful information based on learned intelligence of their interests, search history, and professional network for an enhanced experience
		E.	Unknown
		F.	Not Applicable
			Comments:

84. What best describes your provisioning and architecture for portals?

As-is ✔	To-be ✔		
		A.	Multiple portal solutions exist at different organizational levels; directory and security services are not uniform
		B.	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
		C.	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
		D.	Portals support collaboration and information sharing across extranet and Internet sites in a hybrid on-premises and Web (cloud)-based infrastructure and through federated relationships with trusted partners
		E.	Unknown
		F.	Not Applicable
			Comments:

85. What best describes your integration of line-of-business applications?

As-is ✔	To-be ✔		
		A.	Line-of-business applications and data are delivered through the portal for a few broad-use functions; data is typically read only

		B.	Line-of-business applications are routinely surfaced through the portal and have the capability to write securely to back-end systems and to maintain data integrity; information from multiple applications can be combined in dashboards
		C.	Portals and line-of-business applications are integrated and users can take them offline for changes and secure synchronization later; can access data from these LOB apps across mobile devices; users can combine data from disparate sources into composite applications without IT involvement; IT has the flexibility to create rich client applications and surface them within productivity applications that are used to create and integrate content with the system of record
		D.	None
		E.	Unknown
		F.	Not Applicable
			Comments:

Collaboration

Social Computing

86. What best describes your social media?

As-is ✔	To-be ✔		
		A.	Most content and information delivery is one-way; blogs, wikis, forums, and podcasts are seldomly used, if at all
		B.	Blogs, wikis, and podcasts are used occasionally, but may not be encouraged enterprise-wide; communities, if present, are largely through e-mail or are driven by forums
		C.	Blogs, wikis, and podcasts are used enterprise-wide and compose a significant amount of enterprise content; communities have dedicated,

			actively managed sites that often are customized for specific needs, This Content is accessible through multiple mobile devices.
		D.	Community sites are used with partners across the value chain; social media can be managed for compliance
		E.	Unknown
		F.	Not Applicable
			Comments:

87. What best describes your ability to gather social feedback?

As-is ✔	To-be ✔		
		A.	There is little or no ability to tag, rate, or share bookmarks for any content, social or otherwise
		B.	Social feedback is generally limited to comments in e-mail, forums, or within individual documents
		C.	Rating, tagging, and bookmarking are used broadly to share opinions about all kinds of content and are available from within productivity applications that are used to create content
		D.	Social feedback is incorporated into profiles; users can discover colleagues who share their interests by finding all subscribers to a tag; feedback is used in search and analytics to help determine the best content or resource for a particular need; there is a robust microblogging engine that handles social network updates and comments dynamically
		E.	Unknown
		F.	Not Applicable
			Comments:

88. What best describes your social networking tools?

As-is ✔	To-be ✔		
		A.	There are no enterprise-wide social networking tools; employees may be using various public social networking sites
		B.	Personal profiles are available but cannot be customized; users can publish content on personal shared sites; people can be located based on profile information; the system sorts search results for people by users' social graphs, which can be refined by using metadata; news feeds are typically delivered through RSS or e-mail alerts
		C.	Profiles are highly customizable; personal sites offer organizational, attention management, and public commenting capabilities; social networking and business productivity tools are integrated; enterprise news feeds complement RSS and e-mail alerts. Social networking capability is available via applications on mobile devices.
		D.	Social graph data, user behavior, and social feedback are analyzed to recommend people, groups, and assets; third-party social feeds are exposed within enterprise tools such as personal information management clients; news feeds are generated from relevant line-of-business systems; feeds can be filtered and tuned by end users to improve relevance. social networking is integrated into the main experience of the end-user in an enterprise & is seamless across mobile devices.
		E.	Unknown
		F.	Not Applicable
			Comments:

Collaboration

Project Management

89. What best describes your project planning process?

As-is ✔	To-be ✔		
		A.	Task lists and timelines are maintained by individuals or in shared spreadsheets
		B.	Teams plan, track, and share tasks in lists by using collaboration tools; multiple baselines exist
		C.	Task assignments, task splitting, delegation, and reporting are automated; teams can plan against complex baselines
		D.	Multiple task lists are aggregated and managed against intelligent baselines that have dynamic parameters
		E.	Unknown
		F.	Not Applicable
			Comments:

90. What best describes the way your project teams collaborate?

As-is ✔	To-be ✔		
		A.	Each project has a standalone plan; collaboration is based on file shares, public folders, FTP sites, and e-mail correspondence
		B.	Teams can upload and share documents and files; project workspaces are integrated with desktop productivity applications

		C.	Project tasks and calendars are closely integrated with users' online presence; teams can communicate with a single click; timely updates are available for accurate reporting. Collaboration happens across different mobile devices
		D.	Line-of-business data is available in workspaces and portals; online help and training are widely available
		E.	Unknown
		F.	Not Applicable
			Comments:

91. What best describes project portfolio management in your organization?

As-is ✔	To-be ✔		
		A.	Project proposals are analyzed manually or compared by using spreadsheets
		B.	Portfolios are analyzed in graphical views that include status, resource allocations, and financial details
		C.	Portfolios are analyzed and proposals are selected based on alignment with business goals
		D.	Project and program portfolios are selected by using optimized algorithms; teams routinely use frontier analyses, sensitivity analyses, business alignment assessments, and decision dashboards
		E.	Unknown
		F.	Not Applicable
			Comments:

Unified Communications

Messaging

92. What best describes e-mail protection from malware at your organization?

As-is ✔	To-be ✔		
		A.	Basic e-mail capabilities include anti-spam and minimal or decentralized IT support
		B.	The messaging solution (e-mail and calendar) includes basic anti-virus, anti-spam, and anti-phishing protection
		C.	The messaging solution includes anti-spam, anti-phishing, and multiple-engine anti-virus protection
		D.	The messaging solution supports unified management of multiple anti-virus and anti-spam settings
		E.	Unknown
		F.	Not Applicable
			Comments:

93. What best describes the availability of your messaging system?

As-is ✔	To-be ✔		
		A.	Use of high availability technologies enables messaging system continuity at the server and service levels during outages
		B.	Use of high availability technologies enables continuity of messaging system services during full data center outages

		C.	Seamless, high availability support exists across boundaries (such as data centers and geographies) to ensure service continuity
		D.	None
		E.	Unknown
		F.	Not Applicable
			Comments:

94. What best describes protection and control for your e-mail platform?

As-is ✔	To-be ✔		
		A.	Default encryption exists at the network layer
		B.	The e-mail platform supports message encryption (S/MIME) to enable digital signatures
		C.	The e-mail platform supports advanced, policy-driven message controls that include automatic application of rights protection
		D.	The e-mail platform supports sending, receiving, scanning, and indexing of rights-protected messages among external organizations
		E.	Unknown
		F.	Not Applicable
			Comments:

95. What best describes your strategy for accessing e-mail from anywhere?

As-is ✔	To-be ✔		
		A.	E-mail is available from inside the firewall, but there are no shared calendars or contacts
		B.	Secure, remote, online and offline access to rich mailbox and calendar functionality exists inside and outside the firewall
		C.	Secure, policy-driven access to a unified inbox from PCs, phones, and Web browsers exists inside and outside the firewall
		D.	Advanced policy controls are applied to mobile devices and applications; suppliers and customers have federated calendars; e-mail and contacts are integrated across the enterprise to support collaboration and are available to line-of-business applications
		E.	Unknown
		F.	Not Applicable
			Comments:

96. What best describes your mailbox provisioning?

As-is ✔	To-be ✔		
		A.	IT manages a standalone process to provision inboxes by messaging store (e-mail and voice mail)
		B.	IT manages mailbox provisioning by using a single directory
		C.	Provisioning of user inboxes is driven by business demand, uses a single directory, and provides features based on user needs
		D.	Provisioning of user inboxes occurs automatically based on needs of individual users and spans on-premises and off-premises messaging environments

		E.	Unknown
		F.	Not Applicable
			Comments:

97. What best describes your message archiving solution?

As-is ✔	To-be ✔		
		A.	The data collection process is manual and relies on backup tapes
		B.	Users have separate discovery tools for live and archived mailbox data and must rely on the IT department to conduct searches
		C.	The messaging platform includes integrated search capabilities across multiple mailboxes and supports role-based access and delegation
		D.	Federation is supported across data types and repositories for search and policy management
		E.	Unknown
		F.	Not Applicable
			Comments:

Unified Communications

IM/Presence

98. What best describes your enterprise-level IM solution?

As-is ✔	To-be ✔		
		A.	Public IM is used occasionally for daily business
		B.	Users have secure access to an enterprise-managed online presence and IM infrastructure from inside and outside the firewall; peer-to-peer voice and video communications are based on a single directory
		C.	Online presence, IM, and peer-to-peer voice and video are in place (including multiple-layer anti-malware and contextual content filtering) and are accessible from PCs, phones, and Web browsers
		D.	IM and online presence are federated to suppliers and customers across multiple devices and integrated across line-of-business applications, which enables enterprise networking through expert search
		E.	Unknown
		F.	Not Applicable
			Comments:

99. What best describes your group chat solution?

As-is ✔	To-be ✔		
		A.	Multiple-party IM is managed by the enterprise
		B.	Persistent group chat is available to distributed or multifunctional teams
		C.	IM and online presence are federated to suppliers and customers across multiple devices and integrated across line-of-business applications, which enables enterprise networking through expert search
		D.	None
		E.	Unknown

		F.	Not Applicable
			Comments:

100.   **What best describes your ability to share presence information?**

As-is ✔	To-be ✔		
		A.	Online presence information from within applications is lacking
		B.	Online presence information (automatically refreshed user availability information based on communications, log-on, and calendar activities) is integrated into the e-mail client
		C.	Online presence information and contextual "click to communicate" are integrated into the enterprise productivity and collaboration platform
		D.	IM and online presence are federated to suppliers and customers across multiple devices and integrated across line-of-business applications, which enables enterprise networking through expert search
		E.	Unknown
		F.	Not Applicable
			Comments:

Unified Communications

Conferencing

101.   **What best describes your Web conferencing solution?**

As-is ✔	To-be ✔		
		A.	Web conferencing is used sporadically and is not managed by IT
		B.	Secure Web conferencing is managed by IT, has policy-based access control, uses a single directory, and is available from PCs and Web browsers inside and outside the firewall; an enterprise-wide, standalone audio conferencing service is also managed by IT
		C.	A secure, unified conferencing platform that enables rich audio, video, and data collaboration is managed by IT and is available from enterprise productivity applications; the platform also has a single user interface, a single directory, and is available across organizational boundaries
		D.	Contextual unified conferencing capabilities are integrated and available from within enterprise collaboration and line-of-business applications and across multiple device form-factors.
		E.	Unknown
		F.	Not Applicable
			Comments:

102.   What best describes your audio conferencing solution?

As-is ✔	To-be ✔		
		A.	Audio conferencing is used sporadically and is not managed by IT
		B.	A standalone audio conferencing service is available enterprise-wide and is managed by IT
		C.	A secure, unified conferencing platform that enables rich audio, video, and data collaboration is managed by IT and is available from enterprise productivity applications; the platform also has a single user interface, a

			single directory, and is available across organizational boundaries
		D.	Contextual unified conferencing capabilities are integrated and available from within enterprise collaboration and line-of-business applications and across multiple device form-factors.
		E.	Unknown
		F.	Not Applicable
			Comments:

103. **What best describes your video conferencing solution?**

As-is ✔	To-be ✔		
		A.	Limited video conferencing is available in specialized conference rooms
		B.	Desktop video conferencing is available outside the firewall only through room-based systems, and using methods such as virtual private networking and remote access services that are managed by IT; the end-user experience is disconnected (requires specialized end-user devices or applications)
		C.	A secure, unified conferencing platform that enables rich audio, video, and data collaboration is managed by IT and is available from enterprise productivity applications; the platform also has a single user interface, a single directory, and is available across organizational boundaries
		D.	Contextual unified conferencing capabilities are integrated and available from within enterprise collaboration and line-of-business applications and across multiple device form-factors.
		E.	Unknown
		F.	Not Applicable
			Comments:

Unified Communications

Voice

104. **What best describes your solution for voice over IP communications (VOIP)?**

As-is ✔	To-be ✔		
		A.	Voice communications are based on a legacy TDM PBX (traditonal PBX that is older than 8 years or more) that uses traditional phones; there is no integration with desktop applications
		B.	Voice communications are based on a hybrid telephony infrastructure (IP and legacy time division multiplexing) that has limited integration with PCs and desktop applications
		C.	Voice communications are secure, encrypted, extended to remote and mobile workers using different mobile devices and integrated within enterprise productivity and collaboration platforms
		D.	Voice communications are integrated with other communications modes (such as e-mail, IM/online presence, and conferencing) and with line-of-business applications on a single platform
		E.	Unknown
		F.	Not Applicable
			Comments:

105. **What best describes your access to voice mail?**

As-is ✔	To-be ✔		
		A.	Voice mail is accessible by telephone only. Voice mail is not centralized and exists in individual branches
		B.	Voice mail is available online and offline from the e-mail client but messages are stored separately, there is no unified directory, and messages can be kept private only by caller request
		C.	Voice mail is part of a unified inbox that features single storage and a unified directory; retention and protection policies are enforced by the organization; messages are available as voice or transcribed text and are accessible from PCs, phones, or Web browsers
		D.	Voice mail is integrated with Unified Communications (IM and online presence, conferencing, and messaging) and extends to business processes and line-of-business applications; Voice mail is accessible from PCs, phones, and Web browsers
		E.	Unknown
		F.	Not Applicable
			Comments:

106.   What best describes the voice quality at your organization?

As-is ✔	To-be ✔		
		A.	Use of dedicated circuits and traditional, narrowband codec (G.711) guarantees intelligible speech for connected calls
		B.	Network techniques (quality of service and call admission control) provide preferential treatment for voice traffic within the corporate IP network
		C.	There is an intelligent, adaptive media stack on phone and PC endpoints

			to enable high-quality voice communications even on unmanaged networks (such as the Internet)
		D.	Wideband audio codecs dramatically increase the naturalness of the human voice and the tones, inflections, and other qualities it conveys; the suitability of network conditions for calls is indicated visually (similar to bars on a cell phone)
		E.	Unknown
		F.	Not Applicable
			Comments:

107.   **What best describes your call routing mechanism?**

As-is ✔	To-be ✔		
		A.	Call routing is limited or non-existent
		B.	Call routing between sites is based on lowest cost
		C.	Call routing within an organization is based on identity and online presence
		D.	Call routing is based on identity and online presence, and is extended outside the organization to suppliers, partners, and customers
		E.	Unknown
		F.	Not Applicable
			Comments:

108. **What best describes availability within your voice infrastructure?**

As-is ✔	To-be ✔		
		A.	Redundant hardware provides some resilience within the PBX framework
		B.	Redundant call control servers within a cluster or pool provide resilience when failure occurs at a single point
		C.	Server pools that are split across data centers or replicated provide resilience to data centers when disaster occurs
		D.	Systems are monitored to proactively identify and correct issues that affect service by shifting the load to redundant infrastructure
		E.	Unknown
		F.	Not Applicable
			Comments:

Enterprise Content Management

Information Management

109. **What best describes your document management and repository services?**

As-is ✔	To-be ✔		
		A.	Content is stored in file shares and desktop file systems; there is high reliance on IT to control access
		B.	Managed workspaces exist at the departmental level and are available from individual productivity applications
		C.	Traditional and new media content types are managed consistently in a

			single repository that has integrated workflow
		D.	Centrally managed workspaces support a hybrid on-premises and Web (cloud)-based infrastructure; business content is integrated with automated life-cycle management that includes content creation, discoverability, archiving, and retirement
		E.	Unknown
		F.	Not Applicable
			Comments:

110.   **What best describes your metadata management?**

As-is ✔	To-be ✔		
		A.	Metadata is not centrally managed or applied consistently to content
		B.	Metadata capture is enforced; however, the capture process is manual and labor-intensive
		C.	Metadata is centrally managed and deployed across the business; metadata capture is simplified through preemptive suggestions, or is automated based on location and context
		D.	Metadata includes social tags; search indexing automates promotion of metadata to business applications and processes
		E.	Unknown
		F.	Not Applicable
			Comments:

111. **What best describes your Web and new media management?**

As-is ✔	To-be ✔		
		A.	Web content is managed by a group of specialists who rely heavily on IT for development, maintenance, and support
		B.	Web sites are built using off-the-shelf Web content management platforms; styles and templates are used consistently; content owners are empowered by technology to publish and manage their own information, but most still rely on Web specialists
		C.	Web content is created, published, and managed by business owners who use appropriate publishing workflows to govern review cycles
		D.	Web content is dynamically presented to visitors based on real-time behavior analysis; Web sites are integrated with line-of-business systems to manage and deliver content in both locations
		E.	Unknown
		F.	Not Applicable
			Comments:

Enterprise Content Management

Process Efficiency

112. **What best describes your electronic forms solution and image capturing process?**

As-is ✔	To-be ✔		
		A.	There is no electronic forms capture or management; content is paper-based and manually processed

		B.	Custom solutions developed by IT are used to deliver and manage key forms electronically; form data and scanned paper-based content are stored in a custom data repository
		C.	Users are empowered to create and deploy electronic forms by using visual design tools; data from forms (stored in an open format) and scanned paper-based content are managed as part of an electronic information management strategy; a framework provides leverage for integration of data from forms with line-of-business applications
		D.	All data from forms is captured and validated electronically; paper-based content is scanned and key data is extracted by using character-recognition technology; business processes are automated by using workflows and visual design tools
		E.	Unknown
		F.	Not Applicable
			Comments:

113. **What best describes your human workflow solution?**

As-is ✔	To-be ✔		
		A.	Processes are not formally managed; e-mail is the primary means to manage and share documents and tasks
		B.	The organization uses basic workflow tools to process, review, and approve documents; simple workflow routing is part of the collaborative workspace infrastructure
		C.	The organization gains leverage from visual workflow models and declarative workflow tools to create workflow solutions that have limited integration with line-of-business applications; people can design and validate customized parallel or serial workflows visually as needed, run them manually or automatically, and monitor them in real time

As-is	To-be		
		D.	The organization orchestrates processes with advanced custom workflows, and deploys and integrates line-of-business applications; human and system workflows are integrated for orchestration, exception handling, and automation; people can design workflows by using visual tools, and can reuse workflow patterns in similar scenarios
		E.	Unknown
		F.	Not Applicable
			Comments:

114.   What best describes your approach to document automation?

As-is ✔	To-be ✔		
		A.	Inbound and outbound communications are generated manually; authors use templates to promote consistency, but templates are not centrally managed so output is inconsistent; content reuse is sporadic and requires knowledge of existing information; communication is not managed at the enterprise level as part of an information management strategy
		B.	Inbound and outbound communications are generated by automating productivity applications; IT creates custom connectors for line-of-business applications, so there is heavy reliance on IT to develop, manage, and maintain solutions; templates and output are centrally stored at the enterprise level but not managed as part of an information management strategy
		C.	Inbound and outbound communications are generated by scalable, server-based, automated processes; processes and line-of-business applications are integrated within a framework; templates and output are stored and managed at the enterprise level as part of an information management strategy that provisions core document and records management capabilities
		D.	Business analysts are empowered to develop solutions by using template design tools, workflows, and line-of-business mashup tools; users are

			empowered to generate dynamic, on-demand communications from a range of discoverable templates and content fragments
		E.	Unknown
		F.	Not Applicable
			Comments:

Enterprise Content Management

Compliance

115. **What best describes records management at your organization?**

As-is ✔	To-be ✔		
		A.	Records management is non-existent or is restricted to specialist business functions such as legal, finance, or human resources
		B.	Policy definition occurs at the content repository level and covers retention and disposition of all types of content, including e-mail; reporting occurs manually
		C.	Policy management is based on content type, location, and document libraries, and includes adherence of content used offline; an integrated solution for electronic discovery of information is in place; retention policies and holds on records are automated
		D.	All information created by the organization is managed throughout the content life cycle; policy and compliance are consistently enforced across traditional content, Web content, e-mail, social content, and semi-structured information and across devices.
		E.	Unknown
		F.	Not Applicable

			Comments:

116. What best describes your electronic discovery solution?

As-is ✔	To-be ✔		
		A.	Content exists in multiple repositories and unnecessary content is retained; there is no ability to centrally preserve and analyze content; business relies heavily on outsourcing for review and processing of evidence
		B.	Content is stored in a well-managed repository and disposition rules are appropriately applied; content can be rapidly identified and preserved; business relies heavily on outsourcing for review and processing of evidence
		C.	All information is well managed in accordance with government and industry regulations; content can be rapidly identified and preserved, and the in-house aspect of the discovery process is managed by automated workflow; some content resulting from electronic discovery is initially refined in-house to reduce the volume of content given to external council
		D.	Content that results from electronic discovery can be quickly refined to produce relevant information for use as evidence in court; automated workflow manages the entire discovery process
		E.	Unknown
		F.	Not Applicable
			Comments:

Enterprise Search

Information Access

117. **What best describes your process for indexing content sources?**

As-is ✔	To-be ✔		
		A.	Search capability typically is deployed independently for each content source (desktop and server) for a limited number of users; some Web pages and documents are indexed
		B.	Most unstructured information from intranets, e-mail, and content management repositories is indexed; some structured content from databases, people, and expertise information is indexed
		C.	Unstructured content from the Web, collaborative and content-managed data repositories, databases, and line-of-business applications is indexed; indexing processes incorporate browsing by people and ranking of expertise
		D.	All corporate information assets from structured and unstructured data sources are indexed; a unified taxonomy exists for all key business data
		E.	Unknown
		F.	Not Applicable
			Comments:

118. **What best describes the relevance of your search results?**

As-is ✔	To-be ✔		
		A.	Search relevance is provisioned at the departmental level with limited IT

			engagement or control
		B.	Search relevance is managed by IT, but is not consolidated with the many indexes that exist for different search-enabled business applications; as a result, search relevance can be influenced by how people use and tag search results
		C.	Search relevance is influenced by a blend of indexing and the federation infrastructure; advanced content processing includes the ability to extract entities to add metadata, tags, and structure to unstructured information; as a result, organizations can display best-bets results and provide industry-specific dictionaries
		D.	Custom search requirements and relevance models are defined across multiple roles, business groups, and applications; social tagging and tracking of click-through results improves relevance of search results over time
		E.	Unknown
		F.	Not Applicable
			Comments:

119. What best describes your search-based applications?

As-is ✔	To-be ✔		
		A.	Search capability is not used as an application platform
		B.	Search capability may be used as an application platform, but multiple search platforms are in use or they are separate from the general-purpose search solution
		C.	A single platform provides an organization-wide search experience; structured data is incorporated and exposed in search-driven applications
		D.	All corporate information assets are accessible through search capabilities and search-enabled applications; support for multiple languages exists

		E.	Unknown
		F.	Not Applicable
			Comments:

Enterprise Search

Interactive Experience and Navigation

120. **What best describes the search experience and navigation at your organization?**

As-is ✔	To-be ✔		
		A.	The search experience consists of simple keyword search from a desktop system or browser interface, and includes basic navigation of results that are based on common metadata
		B.	A basic interactive search experience incorporates faceted and filtered information based on common or explicit metadata
		C.	An advanced interactive search experience incorporates faceted information based on extracted metadata and other user experience elements to guide users; the search experience is unified across desktop systems, mobile devices, servers, and Internet searches
		D.	There is a single way to access all information, structured or unstructured, across the organization; search-driven portals and applications provide content targets based on user context and interests and are location aware.
		E.	Unknown
		F.	Not Applicable
			Comments:

Reporting and Analysis

Dashboards

121. **What best describes the ability to search for and access your reports?**

As-is ✔	To-be ✔		
		A.	Users can search for documents but not reports by using simple search functionality, and they must rely on IT for access to data
		B.	Users can search for reports and related unstructured documents, and they have access to data through connections managed by IT
		C.	Users can search for unstructured documents and structured reports based on metadata and report content; IT manages data connections for users; users also can connect to external data sources and combine them in a single report
		D.	Search results are contextual, based on parameters such as user access level, role, and natural language queries; users can filter report content based on keywords
		E.	Unknown
		F.	Not Applicable
			Comments:

122. **What best describes your methodology to create and share scorecards and dashboards?**

As-is ✔	To-be ✔		
		A.	Users make limited use of metrics-based management technology and must rely on IT to create shared dashboards; there are no personal dashboards
		B.	Users create and manage basic team or corporate scorecards that may not use cascading metrics or take a balanced scorecard approach; users create and share information securely through dashboards that require manual updates
		C.	Users create and manage personal or team dashboards and scorecards based on a balanced scorecard methodology that includes dynamic and cascading updates
		D.	Personal, team, and corporate dashboards and scorecards include communication, collaboration, search, and content management capabilities on a single platform that IT manages and users can modify
		E.	Unknown
		F.	Not Applicable
			Comments:

123.   What best describes your ability to deliver data-linked diagrams?

As-is ✔	To-be ✔		
		A.	Diagrams are static and are not linked to data
		B.	Diagrams are linked to data and shared as static Web pages or in PDF
		C.	Diagrams are dynamically linked to data and shared using a Web browser; diagrams display real-time data from one or more sources; data can be refreshed automatically at specific intervals

		D.	Visual mashups from combined diagrams, real-time data, and multiple applications provide compelling, interactive dashboards at the departmental or organizational level
		E.	Unknown
		F.	Not Applicable
			Comments:

Reporting and Analysis

Analytics and Data Mining

124. **What best describes your managed analytics?**

As-is ✔	To-be ✔		
		A.	IT is minimally involved in managing business intelligence applications; end users perform ad hoc queries and data analysis by using spreadsheets or other analysis tools and by pulling data from reports, charts, Web sites, and databases with limited data volume; business logic is expressed by using formulas; multiple copies and versions of data and logic exist and users share their analyses through e-mail or file shares
		B.	IT builds extract, transform, and load packages; data marts; semantic models (online analytical processing cubes); and reports; each application has an independent data mart and model for each locale or subsidiary; IT manages and secures the cubes, models, and data marts, and refreshes the data according to service-level agreements with users; end users perform adhoc data analysis by using spreadsheets or other analysis tools that connect to the model or cube, and they may be required to work with different or multiple models depending on the application or locale; information workers share their analyses through a business intelligence or collaboration portal
		C.	IT builds an enterprise data warehouse and semantic model (online

			analytical processing cube) along with the supporting extract, transform, and load packages; data-cleansing tools; support to multiple languages; and master data management systems; business metrics are centrally defined, and key performance indicators are shared via scorecards and dashboards on the business intelligence portal; sophisticated data management includes partitioning, aggregates, indexing, and the ability to scale up or out; end users perform ad hoc data analysis by using spreadsheet or other analysis tools that connect to the enterprise semantic model or cube
		D.	The organization supports a healthy mix of managed and self-service analytics; IT actively supports self-service analytics by managing the infrastructure on which it runs, and by periodically transferring critical self-service applications to management by IT; parts of the analytics infrastructure are hosted virtually (in the cloud); self-service and managed analytics systems are actively used; business intelligence needs at the enterprise level are met by IT; departments and individuals rely on self-service data analysis
		E.	Unknown
		F.	Not Applicable
			Comments:

125. **What best describes your ability to deliver self-service analytics?**

As-is ✓	To-be ✓		
		A.	IT is minimally involved in supporting business intelligence needs; end users perform ad hoc queries and data analysis by using spreadsheets or other analysis tools and by pulling data from reports, charts, Web sites, and databases with limited data volume; business logic is expressed by using formulas; multiple copies and versions of data and logic exist, and users share their analyses through e-mail or file shares
		B.	IT provides access to common or sanctioned data sources as database

			connections, data feeds, or reports; there is little IT involvement in building actual BI content, but IT monitors usage of business intelligence content, performance, scale, and availability of the portal infrastructure; makes periodic adjustments and also recommends self-service systems when business user requests stretch IT capacity; end users perform adhoc queries and data analysis by using spreadsheet or other analysis tools, and by pulling data from sources sanctioned by IT in addition to other non-sanctioned sources; information workers share their analysis through the business intelligence portal
		C.	IT provisions the business intelligence portal infrastructure with advanced business intelligence capabilities that include search, dashboards, scorecards, alerts, social interaction, browser-based thin-client experience, exception highlighting, guided and predictive analysis, and advanced visualization; end users can perform sophisticated analyses and build feature-rich business intelligence applications by using spreadsheet or other analysis tools; users can easily find data, analyses, and reports on the portal by conducting intelligent searches, and can set up alerts or notifications based on changes to key business metrics. Analytics available across device form-factors (desktop, phones, slates, etc)
		D.	The organization supports a healthy mix of managed and self-service analytics. IT actively supports self-service analytics by managing the infrastructure on which it runs, and periodically transfers critical self-service applications to management by IT; parts of the analytics infrastructure are hosted virtually (in the cloud). self-service managed analytics systems are actively used. business intelligence needs at the enterprise level are met by IT; departments and individuals rely on self-service data analysis and then use social networking tools to collaborate
		E.	Unknown
		F.	Not Applicable
			Comments:

126. What best describes your data mining strategy?

As-is	To-be		

✔	✔		
		A.	IT is minimally involved in supporting data mining needs and the organization has no data mining analysts or automated data mining techniques; end users perform adhoc queries and data analyses by using spreadsheet or other analysis tools, and find data patterns through adhoc data analysis
		B.	IT provisions the infrastructure for data mining activities, and provides access to common or sanctioned data sources as database connections, data feeds, or reports; IT also provisions line-of-business applications with embedded data mining, but there is little IT involvement in building data mining models or performing predictive analysis; data mining analysts use statistical and data mining software to analyze business data and build models to enable future decisions, predict trends, and find correlations in business attributes using a limited set of data mining algorithms and limited data volumes; the analysts then publish results of predictive analyses to business users through reports, spreadsheets, charts, and visualizations; end users consume the results of predictive analyses or embedded line-of-business applications to improve business decisions; end users also rely on self-service data mining tools to perform basic predictive analyses
		C.	In addition to the IT-provisioned infrastructure for data mining activities, support by data mining analysts, and self-service capabilities for end users, is a powerful data mining workbench; the workbench enables data preparation, cleansing, multivariate analysis, and a sophisticated set of data mining algorithms and tuning options (including additional extensibility options such as custom algorithms) to support data mining across huge data volumes
		D.	The data mining infrastructure is provisioned by IT virtually (in the cloud); data mining analysts perform advanced modeling, compare model versions, discover derived attributes, and combine models; end users can make self-service predictions available as functions in the business productivity stack
		E.	Unknown
		F.	Not Applicable
			Comments:

Reporting and Analysis

Report Generation and Distribution

127. **What best describes your report provisioning?**

As-is ✔	To-be ✔		
		A.	IT or a highly technical end user hard-codes a static report from a single data source
		B.	IT manages reporting as a standalone application or function; data is shared from a source library to which end users can apply basic filters
		C.	IT manages reporting components and shared data sets to provide a highly interactive library and reporting environment in which end users can modify or edit source content, change the display, sort, apply filters, and customize reports after they're generated
		D.	Reports can be customized at runtime; end user profile or "point of view" aware reporting
		E.	Unknown
		F.	Not Applicable
			Comments:

128. **What best describes your ability to deliver and share reports?**

As-is ✔	To-be ✔		

		A.	Users request reports by following manual processes that are characterized by rigid separation of tasks and ownership and are largely dependent on IT; end users are minimally involved in delivering or sharing reports and there is little consideration for user needs
		B.	IT manages reporting as a standalone application or function; data is shared from a source library to which end users can apply basic filters
		C.	IT manages reporting components and shared data sets to provide a highly interactive library and reporting environment in which end users can modify or edit source content, change the display, sort, apply filters, and customize reports after they're generated
		D.	Reporting is Web-based and is available across the enterprise across devices; end user profile or "point of view" aware reporting
		E.	Unknown
		F.	Not Applicable
			Comments:

129.   What best describes your reporting notifications and subscriptions?

As-is ✔	To-be ✔		
		A.	End users receive manually delivered reports only; there is no automated notification or subscription
		B.	End users subscribe to reports, but targeted subscription capabilities such as time stamps are limited or non-existent; user specify the device or format in which to receive reports (for example, inbox or e-mail, phone, or Short Message Service text)
		C.	End users subscribe to reports dynamically based on group membership, data values, or filters, for improved context and access to information that is more relevant to their needs; IT configures reporting systems to notify and alert users based on simple data-driven values or rules (such as time

			or another value) and systems can deliver alerts to a number of devices; end users share alerts and subscriptions with others through limited collaboration and social networking
		D.	Sophisticated reporting capabilities are used to generate a master report and then distribute it to a variety of end users as custom subsets of data (data bursting); complex event processing or workflow prompts report generation and distribution
		E.	Unknown
		F.	Not Applicable
			Comments:

130.   What best describes your management and security for reporting infrastructure?

As-is ✔	To-be ✔		
		A.	Users have access to all reports; security is minimal, based on manual push to individual users by the IT department; IT personnel handle management tasks manually
		B.	IT defines roles and permissions to access reports; the reporting system supports time-based snapshots of reports to comply with regulations; reports are also backed up, restored, and stored in a library based on time rules; IT and users maintain security by simple provisioning (such as portal sites and folders)
		C.	IT grants permission to delegate access to reports across boundaries and domains (such as the supply chain); lineage of data sources; users receive reports when data is refreshed; based on their report usage and consumption; when content is relevant to their roles or other specified information; and in response to search criteria. Information about report objects, usage, people, and roles is available
		D.	Security for reports is based on digital rights management that includes

			rules, expiration, and availability windows (for financial and regulatory reasons); lineage of security delegation; compliance lineage: Who saw what data, when, with what permission, given by who…. predefined reports and alerts about report usage and security infractions are available
		E.	Unknown
		F.	Not Applicable
			Comments:

Content Creation

Authoring

131.   What best describes your content options for authoring?

As-is ✔	To-be ✔		
		A.	Content authoring tools provide limited basic formatting; rich media editing is available only in separate applications
		B.	Content authoring tools support rich formatting and rich media editing, and content can be secured with rights management by users
		C.	Content authoring tools deliver advanced formatting. Rich media can be centrally stored, tagged, managed, and made easily available for use in building content deliverables
		D.	Content authoring tools provide contextual formatting options integrated with rich media editing that supports acquisition from or publication to external sources
		E.	Unknown
		F.	Not Applicable

			Comments:

132. What best describes your content creation efficiency?

As-is ✔	To-be ✔		
		A.	Content creation and reuse is inefficient due to limited authoring functionality that includes only basic copy and paste
		B.	Users can intuitively preview, discard, or accept formatting and content; formatting can be saved in templates for reuse
		C.	Content is efficiently reused without loss of context across applications that have different purposes; templates are centrally manageable
		D.	Content sources from line-of-business applications are reliably available within authoring applications
		E.	Unknown
		F.	Not Applicable
			Comments:

133. What best describes your idea capture and retention tools?

As-is ✔	To-be ✔		
		A.	Ideas and information are captured and stored in a mixture of hard copies, e-mail messages, and documents
		B.	Tools are available to capture notes and research gathered by using

			search
		C.	Ideas, notes, and research gathered across Web productivity tools and conversations are easy to find and share
		D.	Ideation tools support the transfer of content from unstructured notes to formal line-of-business systems, to support the development of ideas across groups and systems
		E.	Unknown
		F.	Not Applicable
			Comments:

Content Creation

Multi-device Support

134.   What best describes your consistency of interface across different applications and modes?

As-is ✔	To-be ✔		
		A.	Applications for different tasks have inconsistent user interfaces
		B.	Rich client, Web, and other applications have a consistent user interface paradigm that is optimized for usability and discoverability
		C.	Application user interfaces are customizable at the user and organizational levels for optimal flexibility in user experience and IT control
		D.	Application user interfaces are extensible for seamless integration of capabilities or data into the core interface paradigm
		E.	Unknown
		F.	Not Applicable

			Comments:

135. What best describes delivery options for your applications?

As-is ✔	To-be ✔		
		A.	Applications are delivered in common formats (such as for PC, browser, or phone) for multiple scenarios (such as mobility and reach)
		B.	Key applications support optimized usage scenarios; for example, Web for reach, rich client for responsiveness, and phone for mobility
		C.	Underlying capabilities such as instant messaging, communications, workflow, collaboration, and content management are available in each delivery mode as appropriate
		D.	Rich integration of processes is accessible from within key applications, without context shifting
		E.	Unknown
		F.	Not Applicable
			Comments:

136. What best describes the document integrity?

As-is ✔	To-be ✔		
		A.	Documents that are transferred among users or applications frequently

			show formatting or data loss; fidelity may be lost in final delivery (such as printing or presentation)
		B.	Documents can be delivered or exchanged with high fidelity between all internal and most external users
		C.	Documents can be viewed and edited through optimized modes (such as PC, phone, or browser) without significant formatting or data loss
		D.	Content is produced in line-of-business systems and is rendered by using productivity applications
		E.	Unknown
		F.	Not Applicable
			Comments:

Content Creation

User Accessibility

137. **What best describes the application accessibility?**

As-is ✔	To-be ✔		
		A.	Productivity applications do not support use by people who need accessibility features; standards guideline are not supported
		B.	Productivity applications are designed to facilitate use by people who need accessibility features
		C.	Productivity applications meet guidelines for information and content accessibility in recognized accessibility standards such as Section 508 and Web Content Accessibility Guidelines (WCAG) 2.0 for both PC and web
		D.	A broad ecosystem of third-party extensions further reduces usability challenges for people who require various accessibility accommodations

As-is	To-be		
		E.	Unknown
		F.	Not Applicable
			Comments:

138. **What best describes the content accessibility?**

As-is ✔	To-be ✔		
		A.	There is no significant support for producing standards-based content
		B.	Core productivity applications offer standards-based tools for users to confirm accessibility of content
		C.	New sites meet standards guidelines for supporting assistive technologies in the browser
		D.	Solutions are developed to support process-led checks of user-created content and sites before publication
		E.	Unknown
		F.	Not Applicable
			Comments: