Dell Questions for RiskExec RFQ – *submitted 7/07/25:*

**General**

* When do you envision everything being completed?
* Is the RFP an opportunity to glean a general understand of pricing and determine what is/isn’t possible? Or are you expecting all services in the RFQ to be provided in the $400K budget that was mentioned?
* In response to *“****Company Size & Growth:*** *RiskExec currently employs approximately 30 individuals. We anticipate continued rapid growth, with increasing customer counts, data volumes, and complexity. Vendor solutions must scale efficiently.”* … Could you please quantify the estimated growth you expect and the associated timeline?
* As we engage our custom services team, they may have questions that come up after Monday’s deadline in order to further define the exact services scope. Are we able to work with someone from RiskExec for scoping purposes in the coming weeks?
* Are you currently expecting pricing in the TSA Exit & Migration Projects category, or will that be expected as a secondary exercise at a later time?
* A rough budget of $400K was discussed for these services. Would that be for an entry cost (pay as you go/grow by user), or a 1/2/3 year proposal?
* Are there any current pain points, unmet requirements, or anticipated business changes that could impact your requirements or timelines?
* What metrics/KPIs will define success for each managed service category?
* Is there any documentation, existing runbooks, or policies you can provide for onboarding?

**Cloud & Infrastructure Management**

* How many Azure tenants and subscriptions are currently in-scope for management, and are there anticipated changes in the next 12 months?
* Are there specific naming, tagging, or organizational standards for Azure resources we must follow?
* Can you detail your expectations for Azure cost optimization (e.g., reserved instances, rightsizing, policy enforcement)?
* What is your current process for reviewing and approving cloud billing, and what level of transparency/reporting do you require?
* For DNS and SSL certificate management, which domains, subdomains, and providers (ClouDNS, DNSMadeEasy, SSLS.com) are currently used?
* What is your current backup and disaster recovery architecture—including RPO/RTO targets for different workloads/applications?
* Are there documented incident response and DR playbooks? If not, should the MSP develop these?
* Is there a preferred backup technology or retention schedule, particularly for compliance or regulatory workloads?

**Network and Traffic Management**

* How many applications and regions use Azure Front Door, and are there custom traffic routing or failover requirements?
* Is there a documented topology for Azure Front Door services across your environments?
* Are there any compliance or reporting requirements associated with Azure Front Door management?
* Which types of applications and environments require protection through Sophos WAF, and are specific security policies already defined?
* How many Sophos XG Firewalls are in use, and do you require active support on hardware appliances, virtual appliances, or both?
* Can you specify any compliance frameworks or regulations that network security configurations must meet?
* Are there existing Azure Private Links and Endpoints, or will the MSP recommend and implement new ones?
* Are all DNS zones managed centrally or delegated per application/team? Are DNS changes subject to change management controls?

**Identity & Access Management (IAM)**

* What is the approximate user count for Azure AD/Entra ID, including service accounts and external identities?
* What is your current user provisioning and deprovisioning workflow? Are you using automation tools?
* Which MFA methods do you enforce, and are specific roles excluded?
* Which applications and tools should be integrated via SSO (Rippling, 1Password, others)?
* What is your current endpoint management strategy—number/type of devices, MDM tools in use, and compliance targets?
* Are there custom conditional access or device compliance policies to replicate or redesign?

**Security Monitoring & Response**

* What security operations technologies are currently deployed (Sophos MDR/XDR/EDR, SIEM, others)?
* How many endpoints require MDR/XDR/EDR coverage, and are there hybrid (on-prem/cloud) assets?
* What data loss prevention tools are in place (Nightfall AI, Sophos Cloud Optix)? What are the most sensitive data types?
* What is your expected cadence and format for phishing simulation and security awareness training?
* Are there specific escalation paths, SLAs, or notification requirements for incident response?
* Is 24x7 coverage required for alert monitoring and response, or just incident escalation?
* Do you require documented runbooks for security incidents? Who is responsible for post-incident reviews?

**Patch & Endpoint Management**

* How many endpoints (Windows, macOS, Linux, mobile) and what diversity of device types are supported?
* Can you provide your Patch Management Policy? Are there compliance deadlines or maintenance windows to observe?
* Are there existing tools (like Action1) for patch deployment, or should we propose alternatives?
* What level of detail and frequency do you require for patch compliance and vulnerability reports?
* Are there specific software inventory or license compliance audit requirements?
* Should new endpoint deployment include imaging, software provisioning, and asset tagging?

**Monitoring & Observability**

* What are the service uptime and availability SLAs by application or environment?
* Which monitoring tools are in-place for infrastructure, applications, and user experience? Should these be maintained, migrated, or replaced?
* Are there existing standards for centralized log storage, retention times, and automated alerting?
* What are the expectations for monitoring dashboards, reporting cadence, and notification channels?

**Software License & Application Administration**

* Which applications/licenses are in scope, and what are current counts and contract expiration dates?
* Are there preferred tools or platforms for tracking license usage and optimizing renewals?
* Is license management for renewals, procurement, and budgeting required or just usage monitoring?
* Are there regular audits or reports required for software compliance or vendor licensing?

**Helpdesk & End-User Support**

* What is your approximate end-user count and geographical distribution?
* What hours and channels (phone, email, chat, portal) of support are required for Tiers 1–3?
* What is the onboarding/offboarding process for users, hardware, and software provisioning? Any third-party integration (e.g., Dell leasing)?
* Is there an asset lifecycle management process the MSP needs to interface with or re-design?
* Which collaboration and productivity tools require support (Google Workspace, Slack, Zoom)? Are there integration requirements or restrictions?

**Compliance Support (SOC 2 & Vendor Due Diligence)**

* What is your current SOC 2 compliance status and audit cadence?
* Which documentation artifacts are needed for audit prep (policies, controls, technical evidence)?
* Who in your organization is the primary point of contact for compliance activities?
* Do you have preferred tools for tracking and responding to client/vendor questionnaires?
* How frequently are risk assessments, vulnerability scans, and compliance reviews required, and what are the reporting expectations?

**TSA Exit & Migration Projects**

* What systems or services are currently covered by TSAs, and what are the deadlines for exit?
* Is there a prioritized migration roadmap, or should the MSP advise on migration sequencing?
* Are there known technical, organizational, or data security barriers to migration?
* What is your preferred communication and project management process for migration activities?
* Will MSP resources require on-site presence or involvement for any phase of migration or cutover events?