**Capacity Assessment**

**Rockefeller Central – IT & Cybersecurity Program**

Now that you have a solid blueprint for how your cybersecurity program will look, you need to begin engaging proper project management procedures to prepare for the smooth implementation of the program. Requirements gathering is the next big step, but before that, you need to stop and analyze the capacity requirements for new technologies and controls.

In previous sections, you learned about specific pieces of technology that can enhance your digital security environment, such as centralized identity management, improved logging and monitoring, endpoint security tooling, and backup and recovery controls. While these technologies will strengthen Rockefeller Central's security posture, they also introduce additional load on existing systems. If capacity is not properly planned, new security controls may negatively impact daily manufacturing and administrative workflows.

Because cybersecurity exists to protect workflows—not disrupt them—an upfront capacity assessment is required to ensure that the new IT and cybersecurity controls can operate effectively without degrading performance.

---

**Business Drivers and Growth Assumptions**

A good place to start is to gather major stakeholders and discuss the key drivers of the business.

For Rockefeller Central, leadership identified the following business drivers and assumptions:

- **Expected growth:**
    - Moderate growth over the next 2–3 years, primarily through increased production volume rather than new product lines.
- **New employees:**
    - Four new hires planned within the next 12 months, increasing staff from 10 to 14.
- **Facilities:**
    - No additional facilities planned at this time.
- **Location changes:**

    - No relocation planned.
- **Peak business periods:**
    - Increased production and administrative activity during end-of-quarter and end-of-year periods.
    - Large file transfers related to design documents, manufacturing specifications, and compliance documentation during peak periods.

These drivers indicate steady, predictable growth rather than sudden expansion. Capacity planning can therefore focus on **incremental scaling**, with particular attention to storage, identity services, and backups.

---

**Review of Business Impact Analysis (BIA)**

Next, the Business Impact Analysis was consulted to identify the most critical digital assets supporting Rockefeller Central's operations. The following assets were identified as Tier 1 or Tier 2 systems:

- Domain controller (identity and authentication)
- File servers (shared production and administrative data)
- End-user workstations
- Internet connectivity
- Backup and recovery systems

Performance trends were reviewed over an estimated 30–90 day period using available system metrics and administrative observations.

---

**Current Capacity Observations and Findings**

**Domain Controller**

- **Current state:** One domain controller supporting 10 Windows 11 workstations.
- **Observation:**
    - Authentication and group policy processing are currently stable during business hours.

    - Adding four additional employees will increase authentication requests, login sessions, and group policy processing by approximately 40%.

- **Assessment:**
    - While the domain controller may handle this increase in the short term, it represents a **single point of failure** and leaves little room for additional security services such as advanced logging or IAM integration.
- **Recommendation:**
    - Plan capacity for a **second domain controller (physical or virtual)** within the next 12–18 months to maintain performance and availability.

---

**File Servers and Storage Capacity**

- **Current state:**
    - Two file servers with 1 TB of storage each.
- **Observation:**
    - File servers are already experiencing steady growth due to design files, operational documents, and compliance records.
    - Four additional employees will increase storage consumption and access concurrency.
- **Assessment:**
    - Existing storage capacity leaves minimal buffer for growth, backups, snapshots, or ransomware recovery.
    - Based on the 60–70% utilization rule, each file server should not exceed ~600–700 GB of used space.
- **Recommendation:**
    - Expand file server storage to **at least 3–4 TB total usable capacity** across servers.
    - Separate production data from backup and archival data where possible.
    - Consider cloud-based file storage or hybrid file services for elasticity and offsite resilience.

---

**End-User Workstations**

- **Current state:**
    - Ten mid-spec Windows 11 workstations.
- **Observation:**
    - Workstations currently handle daily workloads adequately.
    - New cybersecurity tooling (endpoint detection and response, disk encryption, logging agents) will add CPU, memory, and disk overhead.
- **Assessment:**
    - Existing systems appear sufficient but are approaching the lower limit of acceptable performance for security-enhanced endpoints.
- **Recommendation:**
    - Ensure new hires receive systems with **equal or higher specifications**.
    - Avoid deploying security agents without validating performance impact through pilot testing.

---

**Internet Connectivity**

- **Current state:**
    - 1 Gbps fiber connection.
- **Observation:**
    - Internet usage is stable, with occasional spikes during file transfers and cloud access.
    - Future cybersecurity initiatives (cloud backups, centralized logging, SaaS security tools) will increase outbound traffic.
- **Assessment:**
    - 1 Gbps is sufficient for current and near-term needs, provided traffic is properly managed.
- **Recommendation:**

    - Monitor peak utilization during end-of-quarter activity.
    - Prioritize critical traffic and schedule large backups outside peak hours.

---

**Backup and Recovery Systems**

- **Current state:**
    - Limited storage headroom due to small file server disks.
- **Observation:**
    - Backups compete for the same storage resources as production data.
- **Assessment:**
    - Backup systems are at risk of exceeding safe utilization thresholds.
- **Recommendation:**
    - Design backup storage to never exceed **60–70% utilization**.
    - Implement offsite or cloud-based backups to handle spikes and ransomware recovery scenarios.

---

**Planning for Spikes and Future Security Controls**

Rockefeller Central experiences predictable spikes during reporting and production cycles. Capacity must be planned as if these spikes were constant conditions.

- Authentication spikes during shift changes and reporting periods
- Storage spikes during document revisions and audits
- Network spikes during backups and cloud synchronization

Where variability exists, **cloud-based scalability and elasticity** should be leveraged, particularly for:

- Backups
- Log storage
- Security monitoring platforms

---

**Capacity Baselines and Planning Outlook**

Based on this assessment, the following baseline principles should guide implementation:

- Target **60–70% sustained utilization** for all critical systems
- Maintain at least **12–24 months of forecasted growth capacity**
- Avoid single points of failure for identity and data storage
- Plan capacity assuming security tooling is always active

---

**Conclusion and Next Steps**

This capacity assessment provides a realistic view of Rockefeller Central's current limitations and near-term needs. The findings should be used directly during the requirements gathering phase to ensure that selected cybersecurity technologies align with existing infrastructure capabilities.

Capacity requirements should be **reassessed twice per year**, with each review forecasting 12 to 24 months ahead. As the business grows, this iterative approach will ensure that Rockefeller Central's IT and cybersecurity program remains effective, scalable, and aligned with operational demands.