Network Segmentation Explained for Program Managers

Zones, traffic, and business dependencies — a practical guide to coordinating stronger security, reliable applications, and informed rollout decisions.

PROGRAM MANAGEMENT | CYBERSECURITY | ENTERPRISE NETWORKS

by Kimberly Wiethoff, MBA, PMP, PMI-ACP

Managing Projects the Agile Way

#NetworkSegmentation #Cybersecurity #CybersecurityProgramManagement #NetworkSecurity #ProgramManagement #SecurityGovernance #RiskManagement #ITLeadership #ManagingProjectsTheAgileWay



Why Segmentation Matters to Your Program

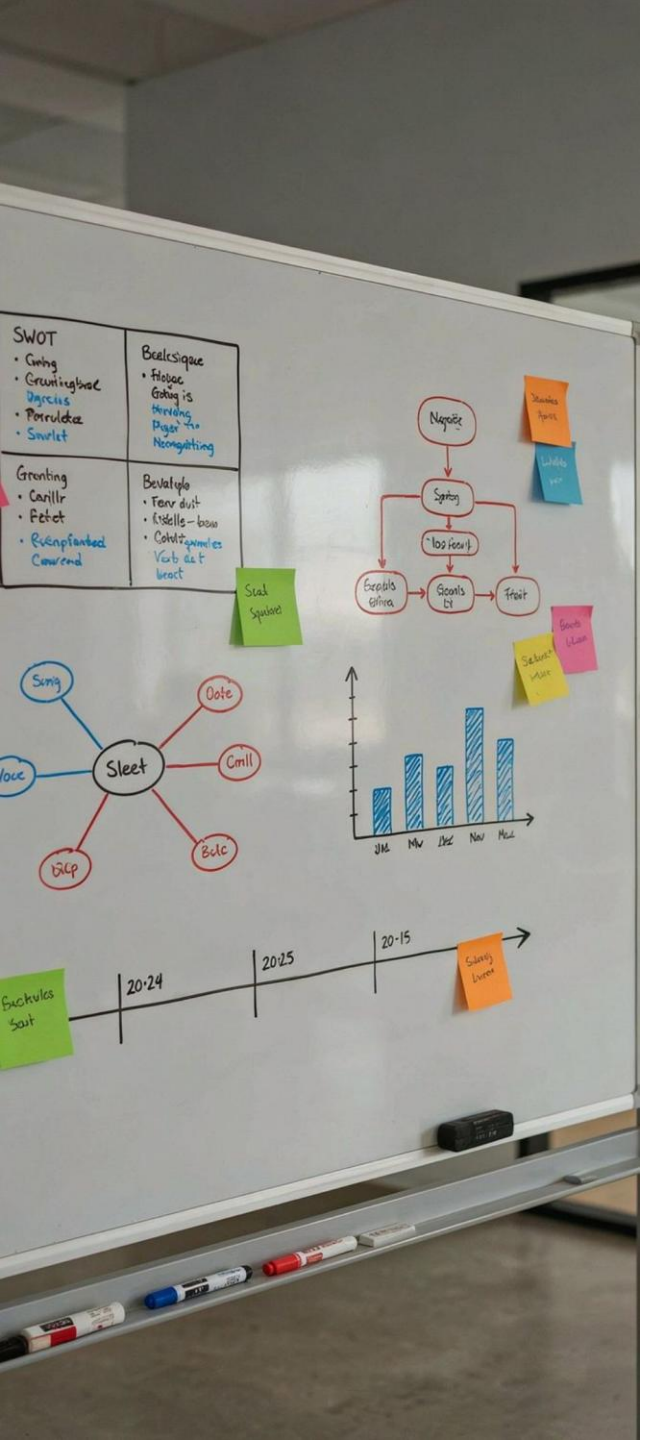
An enterprise network connects the systems people depend on to do their jobs — employee authentication, customer payments, and everything in between. Those same connections can also create pathways an attacker could exploit after compromising a single device or account.

Network segmentation helps organizations **control those pathways** by separating environments and restricting communication between them. For a program manager, delivering segmentation means coordinating security requirements, application dependencies, engineering changes, and business validation.

Your responsibility is to help the organization establish appropriate boundaries while maintaining the services it needs to operate.

Your Core Mission

- Establish appropriate security boundaries
- Maintain operational continuity
- Coordinate across security, engineering, and business teams
- Translate technical controls into trackable outcomes



Start with the Risk You Need to Reduce

Before building the schedule, clarify the problem the program is intended to solve. The right objective shapes everything that follows — scope, dependencies, and acceptance criteria.

Separate Environments

Isolate production from development to prevent accidental or malicious cross-contamination.

Restrict Third-Party Access

Limit vendor and partner connectivity to only the systems and paths required for their specific function.

Protect Sensitive Data

Shield customer databases and regulated data stores from broad internal access.

Limit Lateral Movement

Prevent attackers from moving freely between user devices and critical infrastructure after initial compromise.

Defining the Objective

Ask the Right Questions First

> Only approved application services and authorized administrative pathways should be able to connect to the customer database.

That statement identifies a protection requirement the technical team can design and test — and gives the program manager a basis for tracking outcomes. Bring this discipline to every objective.

- → Which business services or data are we protecting?
- → Which access paths create unacceptable exposure?
- → What communication must remain available?
- → What evidence will demonstrate that the control works?
- → Who can accept any remaining risk?

Direct these questions to the sponsor and security architect. Their answers should shape the charter, roadmap, and implementation priorities.

Understand the Language of Segmentation

You don't need to configure firewall rules to lead this program. You do need enough technical fluency to recognize dependencies and ask productive questions in architecture reviews and delivery standups.

Term	Meaning	Why It Matters to Delivery
Security zone	A grouping of resources with defined security requirements	Establishes scope, boundaries, and ownership
East-west traffic	Communication between systems within an environment	Reveals application dependencies and lateral movement paths
North-south traffic	Communication entering or leaving an environment	Identifies external connections and ingress/egress requirements
Firewall policy	Rules permitting or denying communication	Requires review, testing, approval, and ongoing maintenance
Lateral movement	An attacker moving from a compromised resource toward others	Explains the primary risk segmentation is designed to reduce
Application dependency	A system or service an application relies on to function	Overlooked dependencies cause disruption during enforcement

A VLAN can support separation — but it doesn't guarantee restricted access. Always ask architects *where* controls are enforced and *how* they will be validated.

Chapter 2

Follow the Complete Business Workflow

Imagine a claims-processing application. Employees access a web interface; the web server talks to an app server; the app server reads and writes to a database; the app exchanges data with a payment service. Those are the visible connections. But others are equally critical.



Identity & Authentication

Identity services authenticate users and service accounts. Block this, and the application cannot confirm who is accessing it.



DNS & Discovery

Systems rely on DNS to locate one another. Interrupting DNS silently breaks connections that otherwise appear correctly configured.



Monitoring & Backups

Monitoring collects health data; backup platforms protect records. Both must be accounted for in permitted-flow design.



Scheduled Jobs & Admin Access

Batch jobs, file exchanges, and administrative pathways may only run at off-hours — but they're just as essential to service continuity.

Planning unit: The complete business service — including every supporting dependency — not just the primary user transaction.

Chapter 3

Turn Traffic Data into Validated Requirements

Observed communication is a discovery input, not a final answer. A connection might support a critical workflow, an obsolete integration, a temporary workaround, or unwanted activity. Automatically preserving every observed connection carries unnecessary access into the new design.

Bring application owners and technical specialists together to **validate the business purpose** of every required flow before it enters the approved policy.

Assign owners to every unresolved dependency and include their resolution dates in the integrated plan. Unowned items become blockers.

Information	Decision It Supports
Source and destination	Which resources need to communicate?
Port, protocol, and direction	What specific communication is required?
Business purpose	Why should this connection remain available?
Frequency or trigger	When does the dependency become active?
Accountable owner	Who can validate the requirement?
Exception status	What uncertainty or exposure remains?

Chapter 4

Plan for the Business Calendar

A short observation window may capture daily transactions while missing month-end reconciliation, quarterly reporting, disaster recovery tests, or scheduled vendor maintenance. Each of these involves distinct communication flows that may not appear in standard traffic data.

Ask application owners: *What happens outside ordinary daily operations?*

For example, a finance application may pass standard transaction testing — then fail when its month-end batch job connects to a reporting service omitted from the approved policy.

When a Gap Is Discovered, Choose One

1. **Extend testing**

   Cover the missed scenario before enforcing the policy.

2. **Move the wave**

   Shift the application to a later deployment wave.

3. **Approve a narrow exception**

   Document scope, risk, owner, and expiration explicitly.

Chapter 5

Build Readiness into Every Rollout Wave

Organize implementation waves around both **risk and readiness**. An application's business importance does not make it a suitable first pilot — complexity, recovery options, and dependency confidence matter equally.

Ownership

Named application, infrastructure, security, and support owners are confirmed and engaged.

Dependencies

Critical flows are reviewed; discovery gaps are documented and owned.

Business Validation

Representative transactions and integration tests have been executed successfully.

Security Validation

Tests confirm that selected unauthorized paths are blocked as intended.

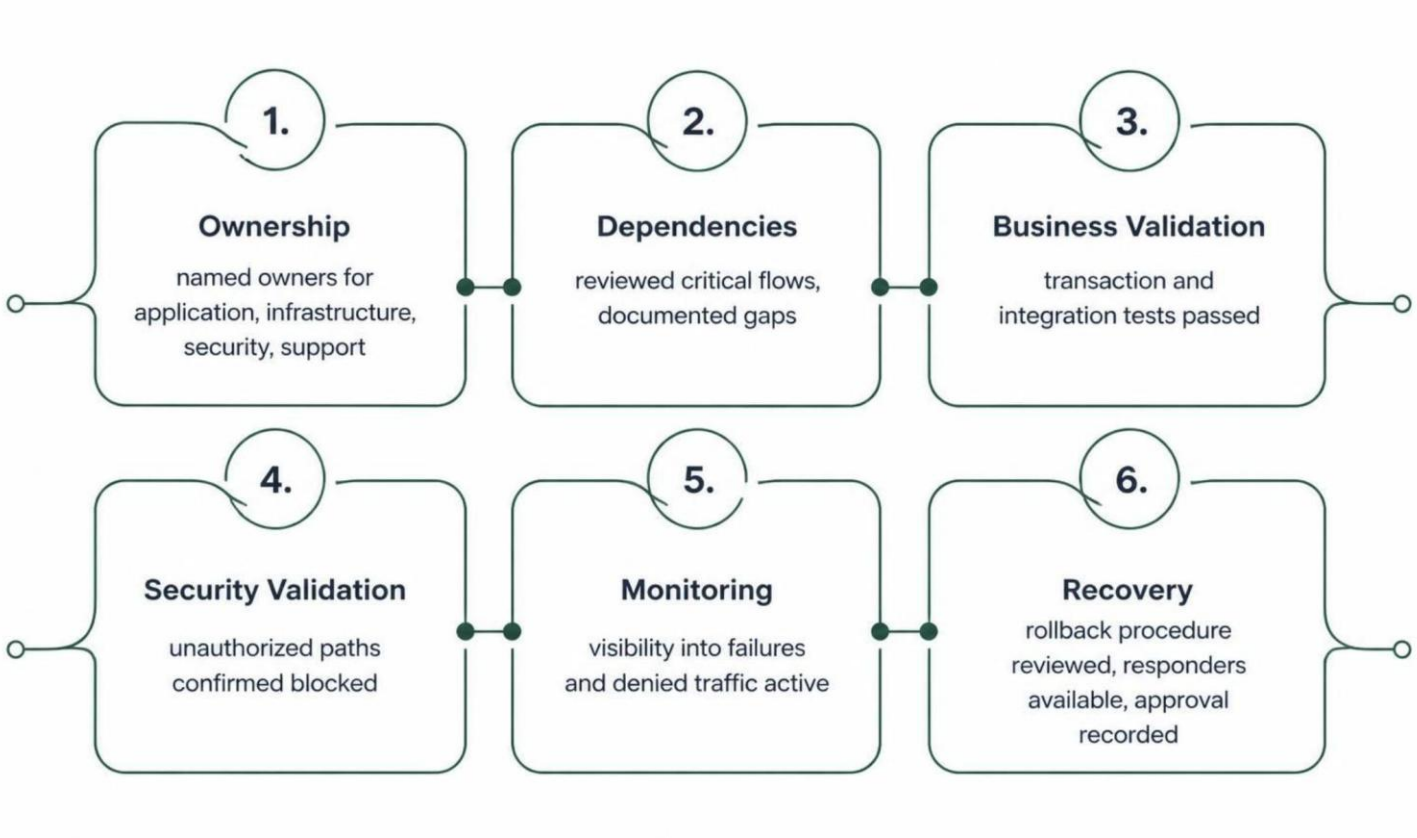
Monitoring & Recovery

Visibility into denied traffic and service health is active; rollback procedure is reviewed and responders are available.

Test both sides: legitimate work continues *and* inappropriate communication is restricted. One without the other is incomplete validation.

Readiness Criteria

What "Ready" Actually Looks Like



Treat each criterion as a gate. Waves that do not meet readiness criteria should be deferred — not forced through on schedule pressure alone.

Chapter 6

Handle Exceptions with Accountability

Legacy applications and incomplete discovery will create legitimate reasons for exceptions. That is expected. The risk lies not in granting exceptions but in **losing track of them**.

A broad rule introduced to meet a deadline can become a lasting exposure if nobody owns its removal. Track exception closure alongside implementation progress, and report aging exceptions to leadership explicitly.

Every Exception Record Must Include

Scope & Rationale

What is permitted, and why the standard control cannot apply now.

Owner & Approving Authority

Named individuals who accepted the tradeoff on record.

Remaining Risk

What exposure exists while the exception is active.

Expiration & Remediation Plan

A specific review date and the path to closure.

Chapter 7

Report Outcomes Leaders Can Assess

Completed rule changes show activity. Leadership needs evidence of **protection and service stability** — not just task completion. Present measures alongside the decisions they require.

Validated Dependencies

Applications with all critical flows reviewed and approved by named owners.

Controls Tested

Security validations confirming unauthorized paths are blocked as designed.

Workflows Passing

Business transactions confirmed successful post-enforcement.

Aging Exceptions

Open exceptions past their review date — each requires a named decision.

If a wave is delayed because application owners have not validated critical flows, make that dependency and its business impact explicit in your status report — not buried in a task list.



The Question to Carry into Every Review

What must remain connected for the business to operate, what should be restricted, and how will we prove both outcomes?

This question is the program manager's compass throughout delivery. It bridges the technical work of firewall policy with the business accountability of service continuity and security assurance. Keep it at the center of every stakeholder review, wave gate, and status report.

About the Author

Kimberly Wiethoff, MBA, PMP, PMI-ACP



Kimberly is a Senior Program Manager with deep experience in enterprise technology transformation, regulated cybersecurity delivery, PMO governance, and Agile program execution.

Through **Managing Projects the Agile Way**, she shares practical approaches to managing complex initiatives, coordinating technical teams, and making informed delivery decisions in high-stakes environments.

Visit Managing Projects the Agile Way

Areas of Expertise

- Enterprise technology transformation
- Regulated cybersecurity program delivery
- PMO governance & Agile execution
- Cross-functional team coordination
- Stakeholder communication & risk reporting