A GRC Professional's Guide to Network Ports: Risk and Compliance Implications

Document Version: 1.0
Audience: GRC Analysts, IT Auditors, Compliance Officers
Purpose: To provide a reference for assessing the risk and compliance posture of systems based on observed open network ports.

Introduction

For Governance, Risk, and Compliance (GRC) professionals, understanding network ports is not about the deep technical mechanics, but about **understanding the risk and compliance implications of the services running on them.** An open port represents a potential door into a system. Your role is to identify if that door is necessary, properly secured, and compliant with organizational policy and regulatory frameworks.

This guide categorizes common ports by their typical risk level and explains what finding them open might mean from a GRC perspective.

High-Risk Ports: Immediate Attention Required

These ports are frequently associated with critical vulnerabilities, unauthorized access, or data exfiltration. Their presence, especially if unnecessary, often represents a severe compliance failure.

Port	Protocol	Service	GRC Concern & Compliance Mapping
21	TCP	FTP (File Transfer Protocol)	**Cleartext credentials & data.** Violates confidentiality principles in **NIST CSF (PR.DS-2)**, **PCI DSS (4.1)**, and **GDPR (Art. 32)**.
22	TCP	SSH (Secure Shell)	**Critical for remote admin.** However, weak passwords/policies violate **CIS 5.2/5.4**. Should not be exposed to the entire internet.
23	TCP	Telnet	**Extremely High Risk.** All communication, including logins, is in cleartext. **Never acceptable** in a modern environment. A clear violation of any security policy.
135	TCP	MSRPC (Microsoft RPC)	Provides a large attack surface on Windows systems. Can be used for lateral movement. Often unnecessary.

139, 445	TCP	NetBIOS, SMB (Server Message Block)	Critical for Windows file/printer sharing but notoriously vulnerable (e.g., EternalBlue). Can lead to credential theft and ransomware propagation. Violates **CIS 9.1** (Limit open ports).
3389	TCP	RDP (Remote Desktop Protocol)	A prime target for brute-force attacks. Exposing this to the internet is extremely high risk. Requires strong controls (MFA, NLA) to be compliant.

Medium-Risk Ports: Review for Business Necessity & Security

These ports are common for essential services but can be leveraged in attacks if misconfigured, unpatched, or unnecessary.

Port	Protocol	Service	GRC Concern & Compliance Mapping
25	TCP	SMTP (Simple Mail Transfer Protocol)	Should only be open on designated mail servers. Can be used for spam relay if misconfigured.
53	TCP/UDP	DNS (Domain Name System)	Essential but can be used for amplification attacks (UDP) or zone transfers (TCP) if improperly secured.
80	TCP	HTTP (Hypertext Transfer Protocol)	**Web traffic.** The risk depends entirely on the security of the underlying web application (OWASP Top 10).
443	TCP	HTTPS (HTTP Secure)	**Encrypted web traffic.** The standard for all web traffic. Check certificate validity and supported encryption protocols.
1433	TCP	Microsoft SQL Server	Database access. Should never be exposed to untrusted networks. Access must be tightly controlled and logged.
3306	TCP	MySQL Database	Database access. Same concerns as MS-SQL. Violates **PCI DSS 2.2.4** if exposed unnecessarily.
5432	TCP	PostgreSQL Database	Database access. Same concerns as other databases.

5900+	TCP	VNC (Virtual Network Computing)	Often has weak authentication. Traffic is often unencrypted. Use a secure alternative like SSH tunneling.

Low-Risk / informational Ports

These ports are generally harmless but can provide valuable information to an attacker for reconnaissance.

Port	Protocol	Service	GRC Concern & Compliance Mapping
135	UDP	Ephemeral Ports for RPC	Typically not a direct risk but part of normal OS operation.
161, 162	UDP	SNMP (Simple Network Management Protocol)	**Can be high risk if misconfigured.** Default community strings (public/private) are a severe information disclosure risk, violating **CIS 4.3**.
389	TCP	LDAP (Lightweight Directory Access Protocol)	Directory services access. Cleartext by default. LDAPS (636) is preferred.
636	TCP	LDAPS (LDAP over SSL)	Encrypted directory access. The secure way to run LDAP.

The GRC Audit Process for Network Ports

1. **Discover:** Use tools like nmap (as in Lab 1) to generate a list of open ports on a target system.

```
nmap -sT -O <target_ip>
```

2. **Inventory & Compare:** Compare the list of discovered open ports against the **approved baseline** or **allowed services list** defined in the organization's security policy. This is a direct test of **CIS Control 9** (Limitation and Control of Network Ports).

3. **Assess:**

    - **Business Justification:** Is there a documented business need for this service/port to be open?

   - **Configuration:** Is the service configured securely? (e.g., is it running the latest version? Are default credentials changed? Is encryption used?).
   - **Exposure:** Is the port exposed only to the necessary network segments, or is it open to the entire world?
4. **Map to Frameworks:** Document the finding within the context of compliance.
   - **Finding:** "Unencrypted Telnet service (port 23) detected on server X."
   - **Risk:** High - Credential interception, unauthorized access.
   - **Compliance Violation: NIST CSF PR.DS-2** (Data-in-Transit Protection), **PCI DSS 4.1** (Encrypt transmission of cardholder data), **CIS 9.1** (Limit open ports).
5. **Recommend:** Recommend action based on risk.
   - **High Risk:** Disable the service immediately.
   - **Medium Risk:** Harden the configuration, apply patches, and restrict network access.
   - **Low Risk:** Confirm business justification and document.

Conclusion

For a GRC professional, a network port scan is not the end goal it is the starting point for a crucial conversation about risk and compliance. By understanding the "why" behind the port, you can effectively advocate for secure configurations, validate controls, and ensure the organization's network posture aligns with its policies and regulatory obligations.

Remember: The principle of **Least Functionality** (NIST SP 800-179) is key: any system should only have the ports and services open that are essential to its business function. Your job is to enforce this principle.