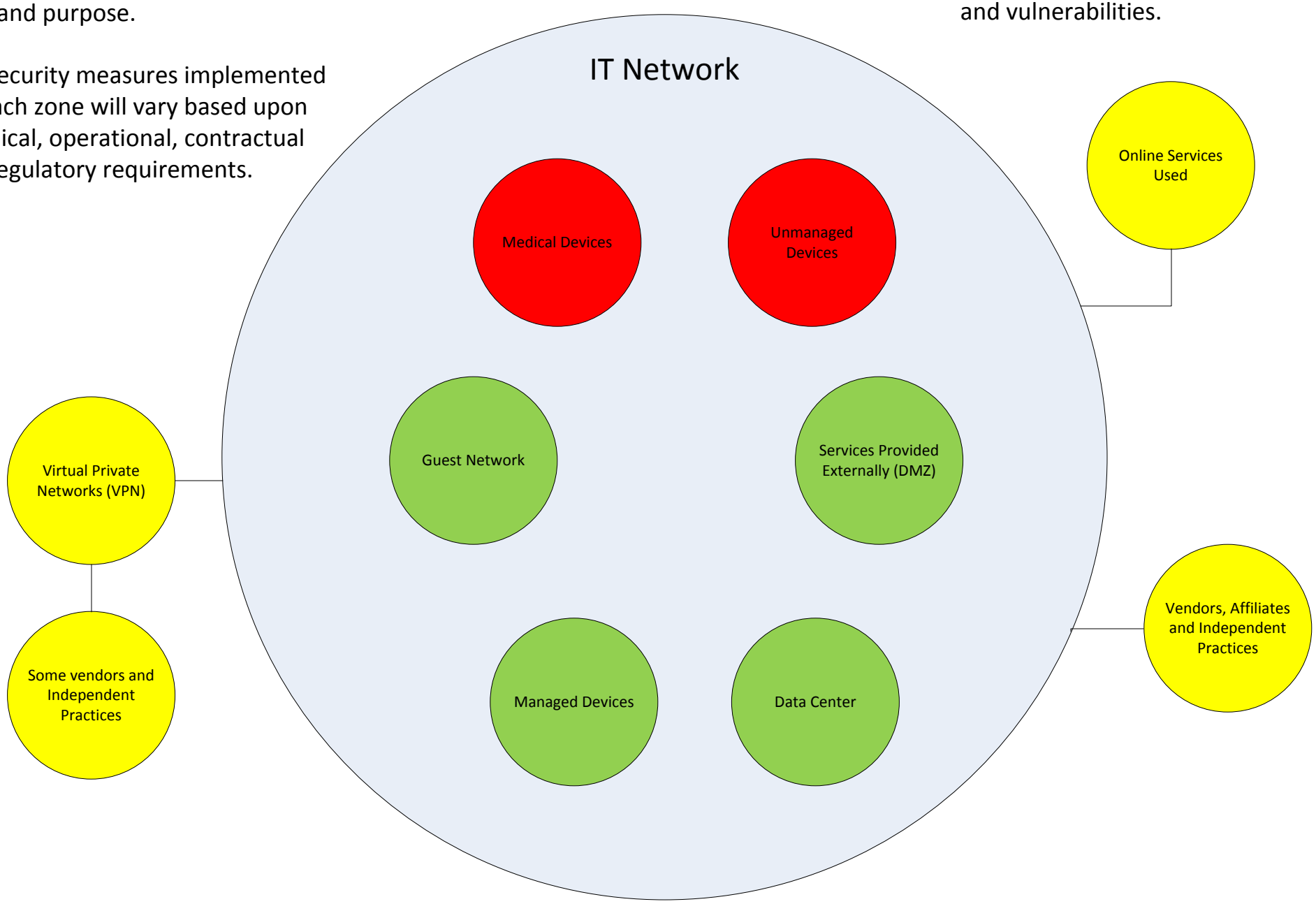
The IT network will contain several zones with devices of a similar risk level and purpose.

The security measures implemented for each zone will vary based upon technical, operational, contractual and regulatory requirements.

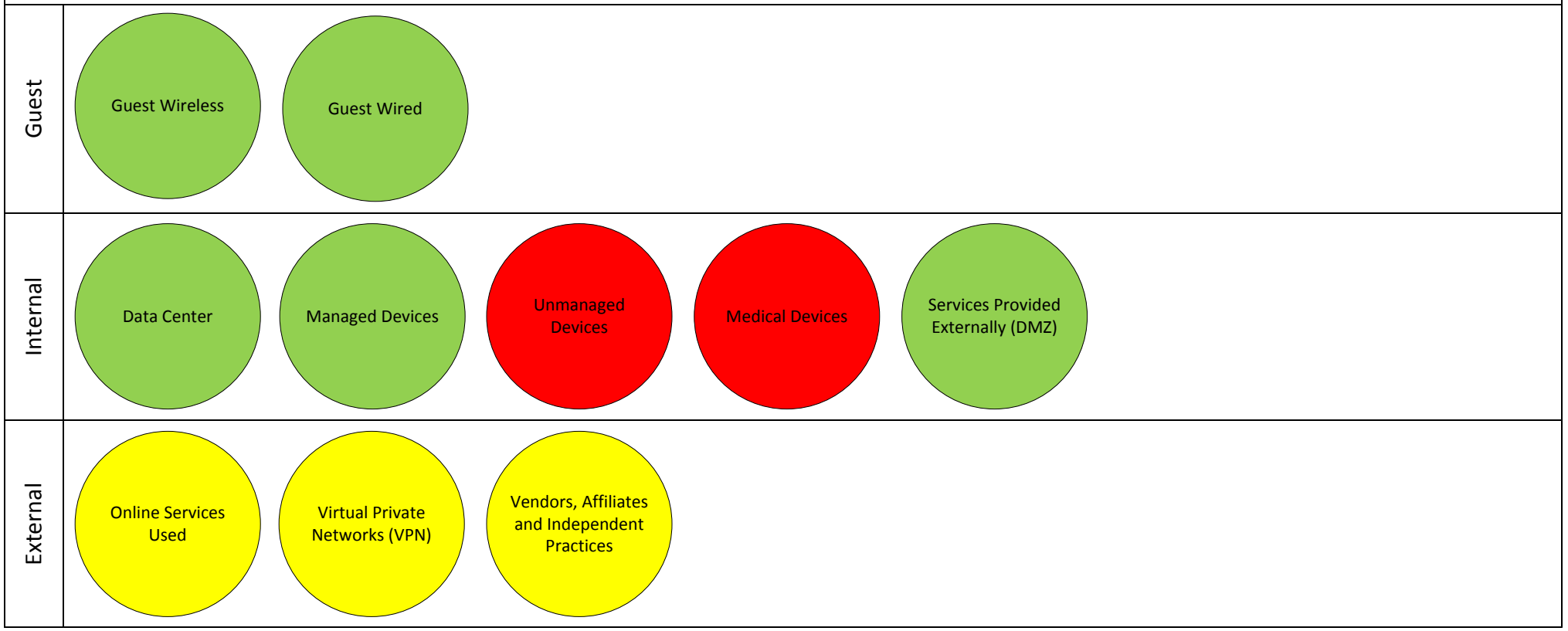
Colors indicate the level of risk given the current tools, processes and vulnerabilities.



IT Network

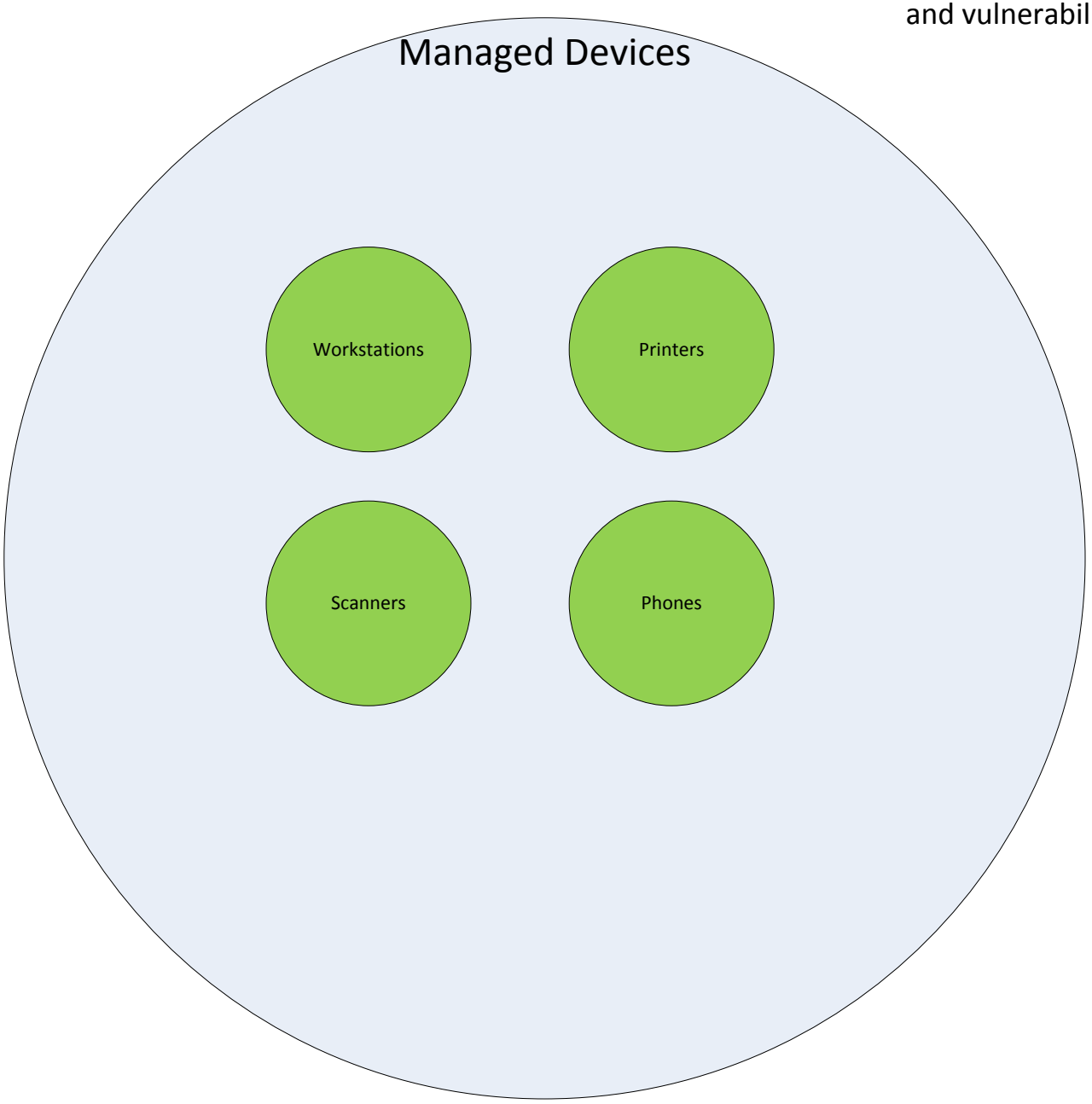
Colors indicate the level of risk given the current tools, processes and vulnerabilities.

The IT network will contain several zones with devices of a similar risk level and purpose. The security measures implemented for each zone will vary based upon technical, operational, contractual and regulatory requirements.



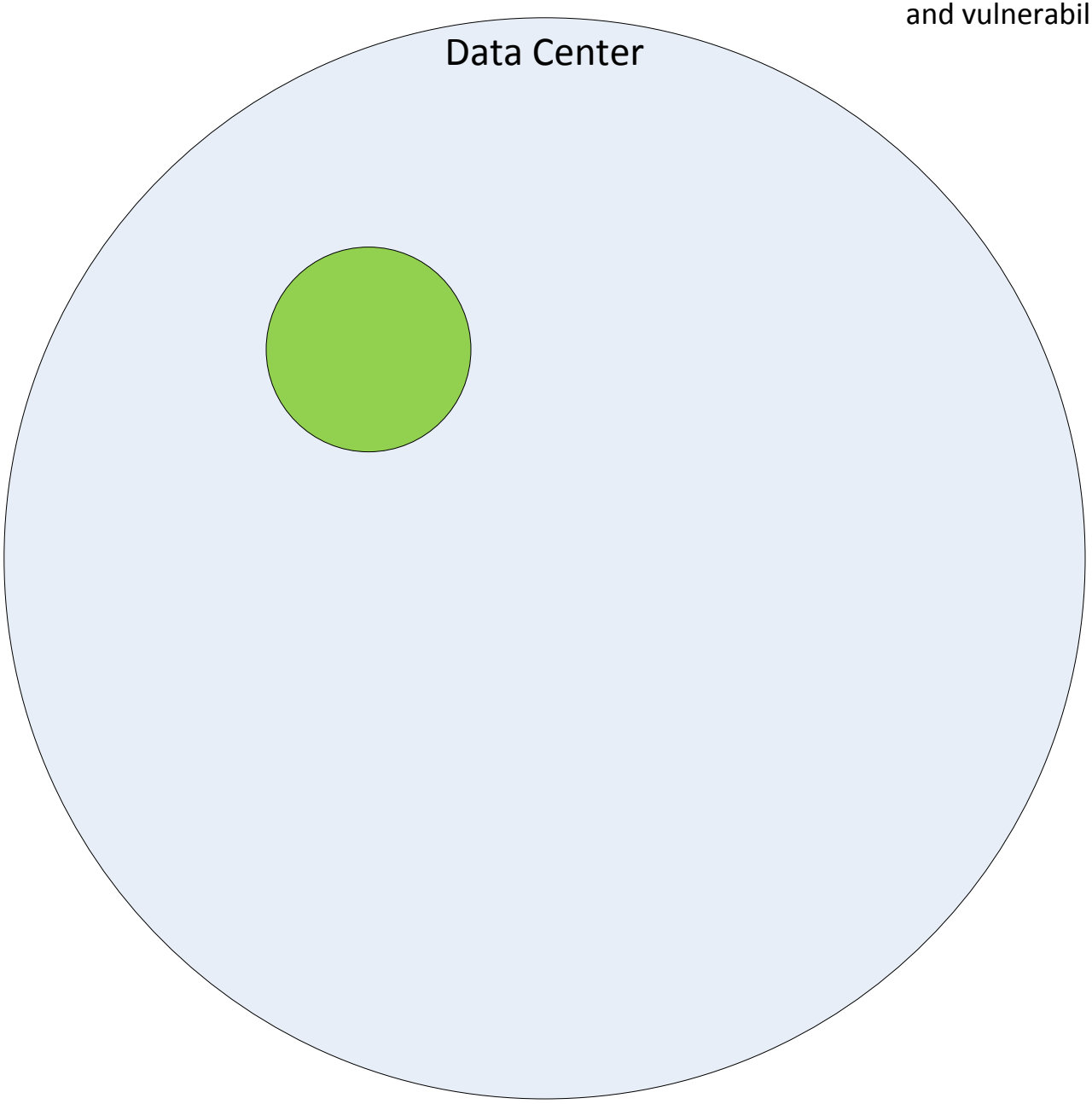
Back to Overview

Colors indicate the level of risk given the current tools, processes and vulnerabilities.



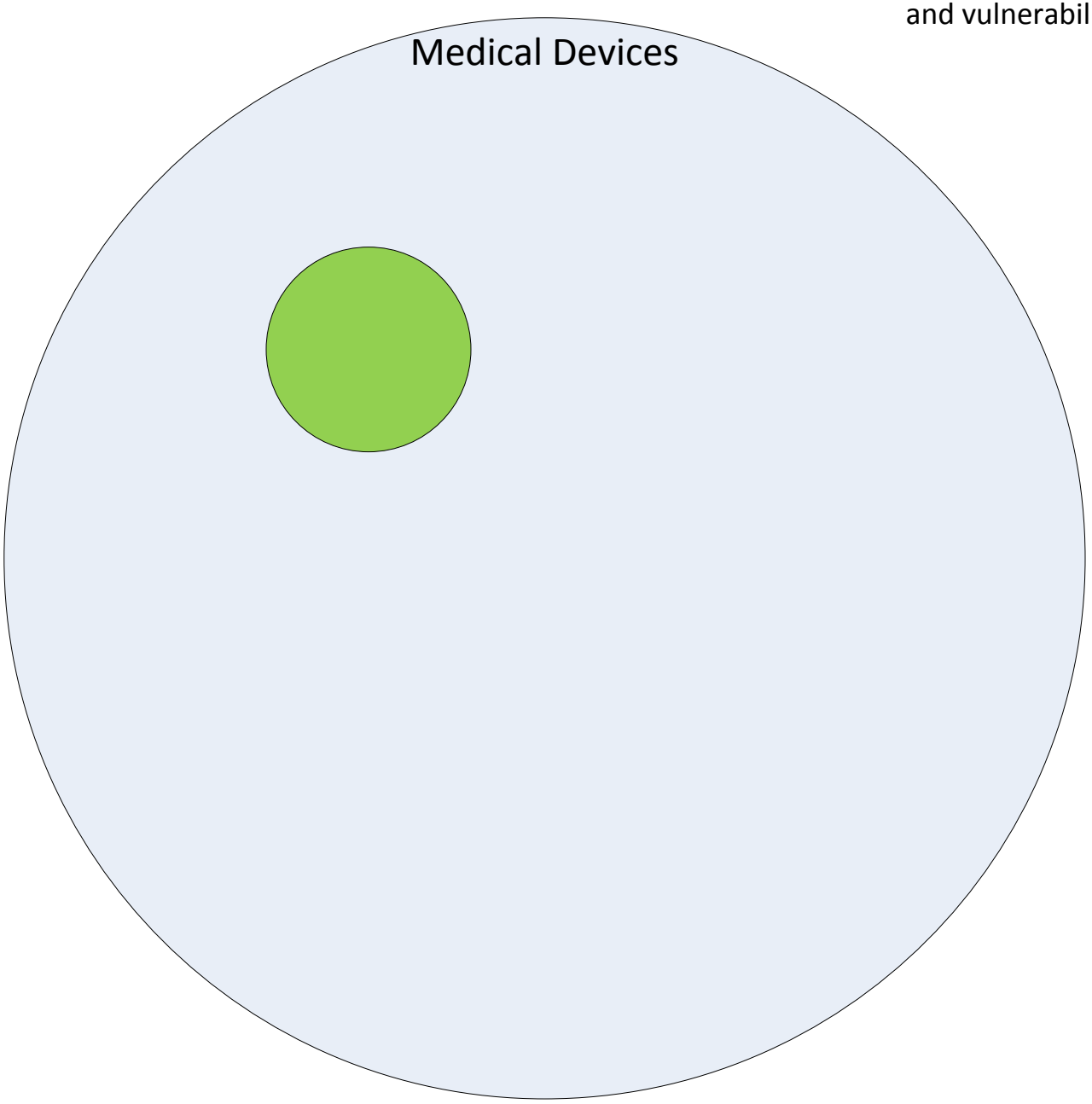
Back to Overview

Colors indicate the level of risk given the current tools, processes and vulnerabilities.



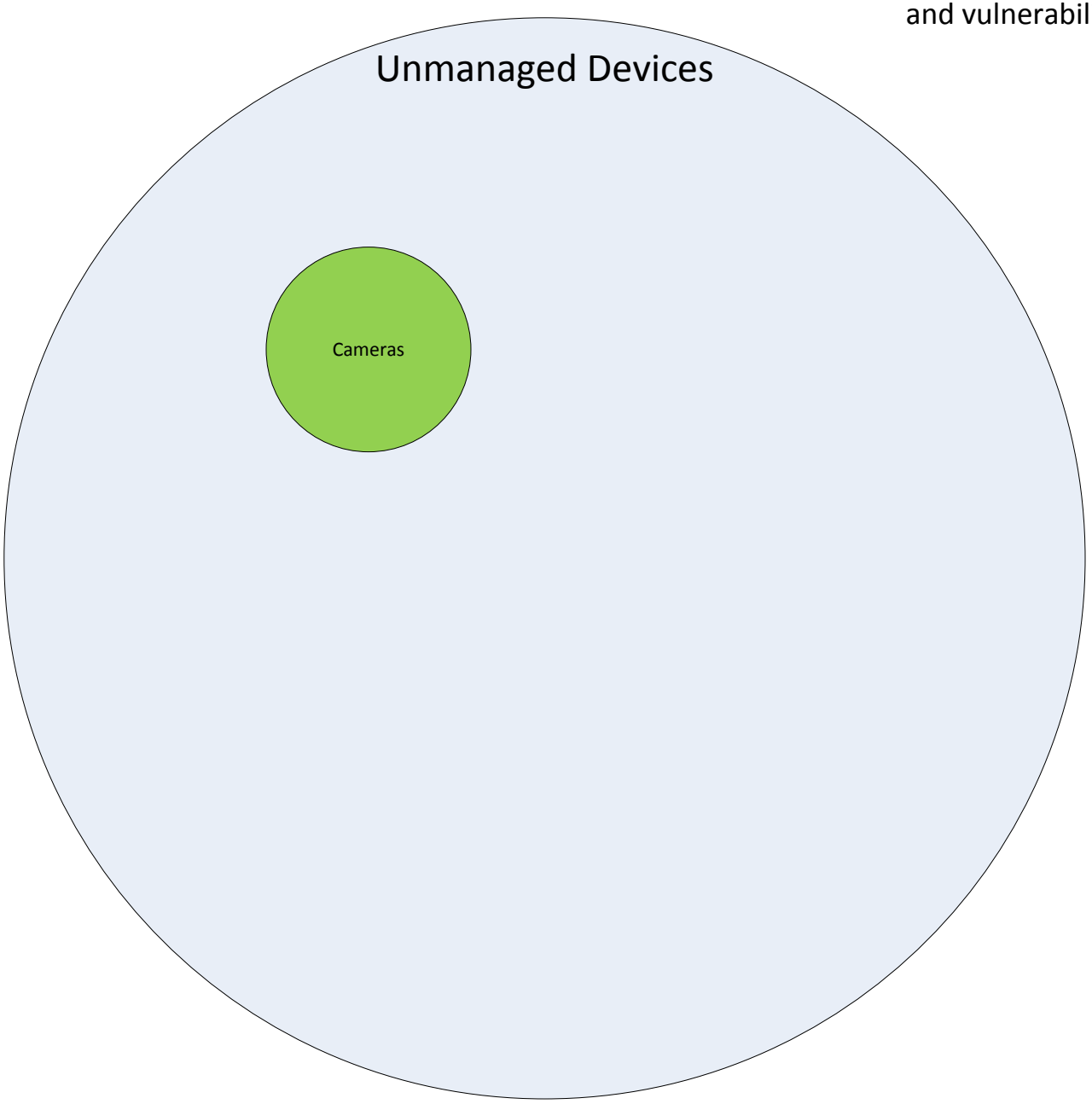
Back to Overview

Colors indicate the level of risk given the current tools, processes and vulnerabilities.



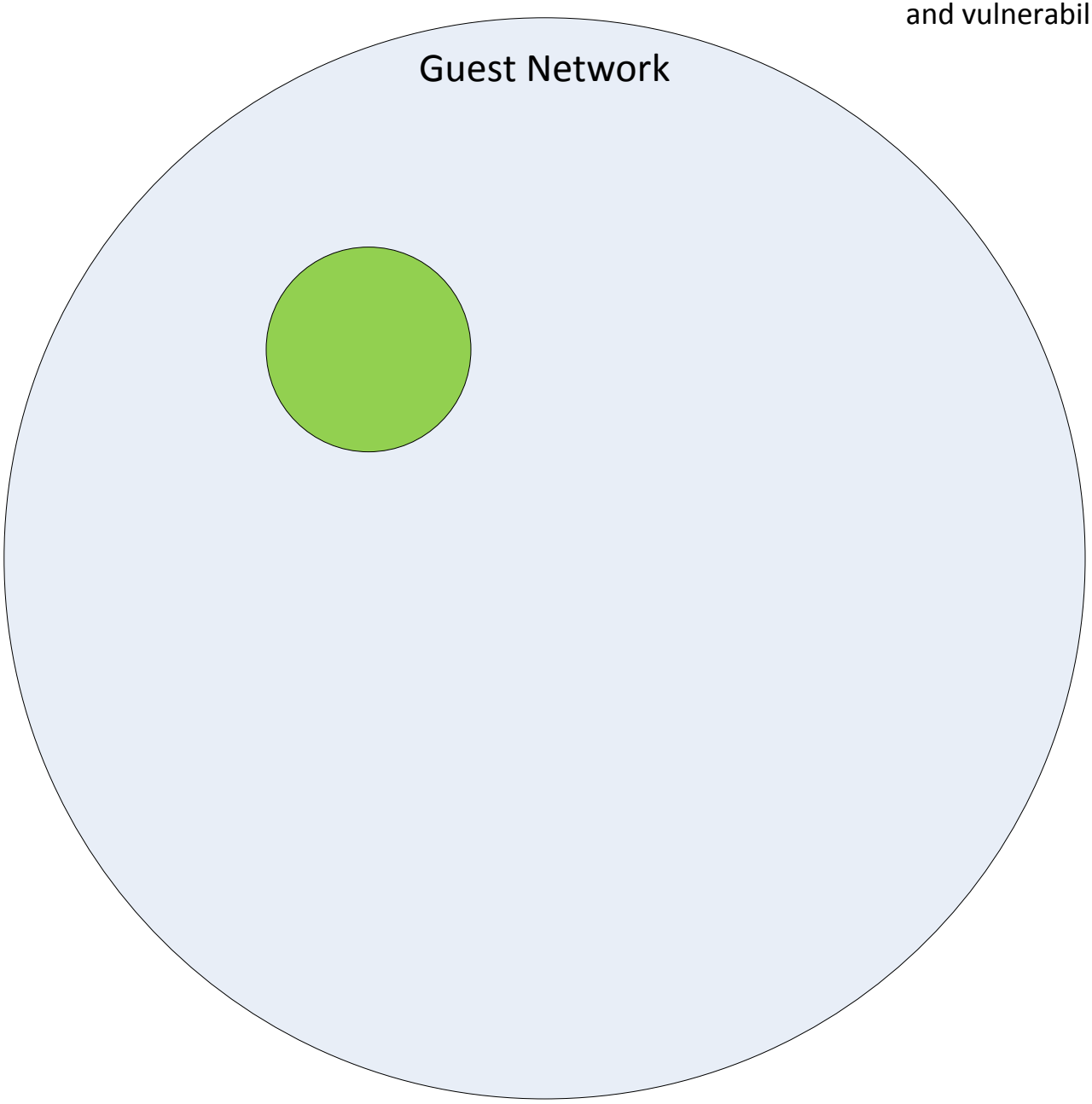
Back to Overview

Colors indicate the level of risk given the current tools, processes and vulnerabilities.



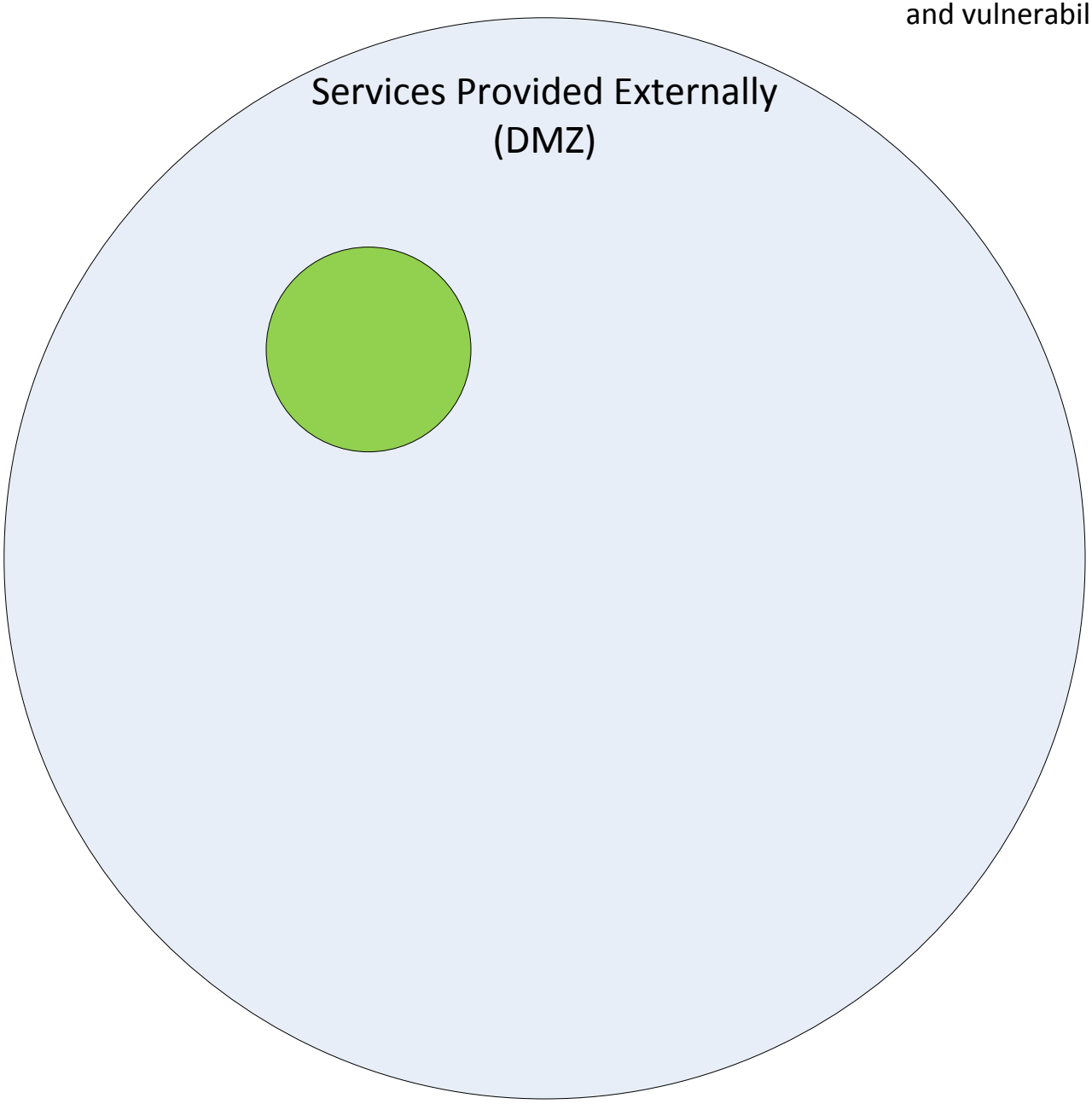
Back to Overview

Colors indicate the level of risk given the current tools, processes and vulnerabilities.



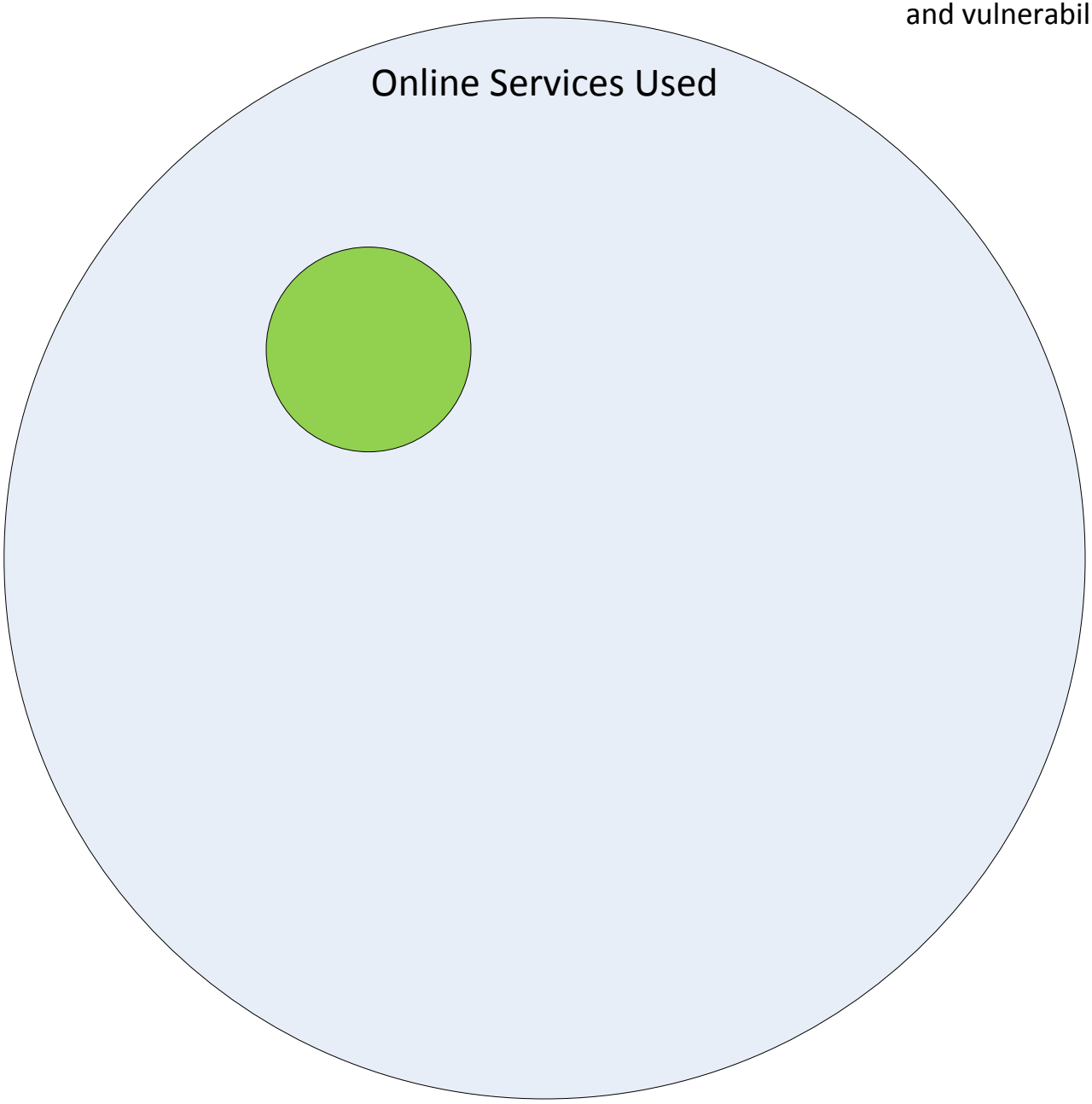
Back to Overview

Colors indicate the level of risk given the current tools, processes and vulnerabilities.



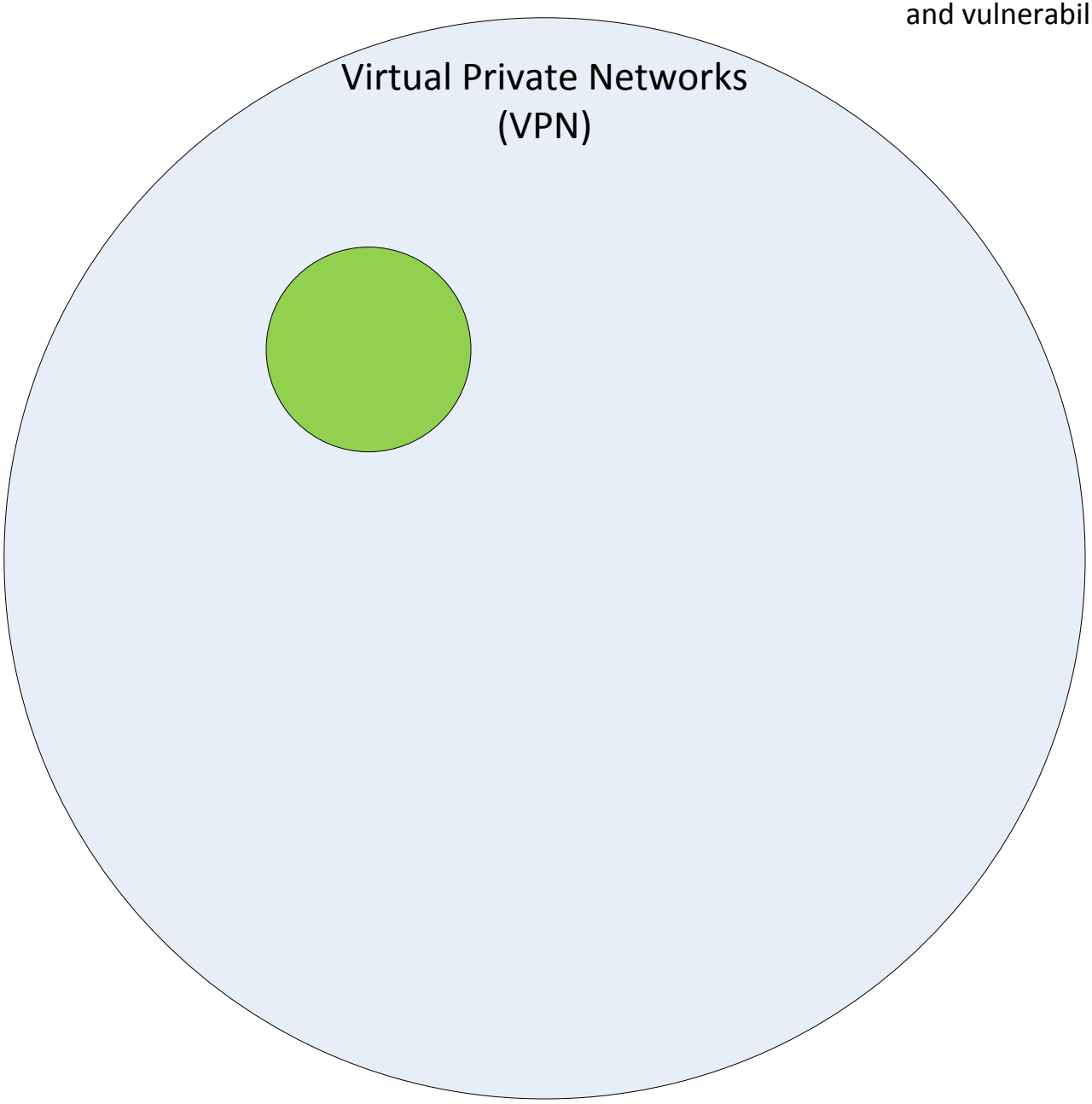
Back to Overview

Colors indicate the level of risk given the current tools, processes and vulnerabilities.



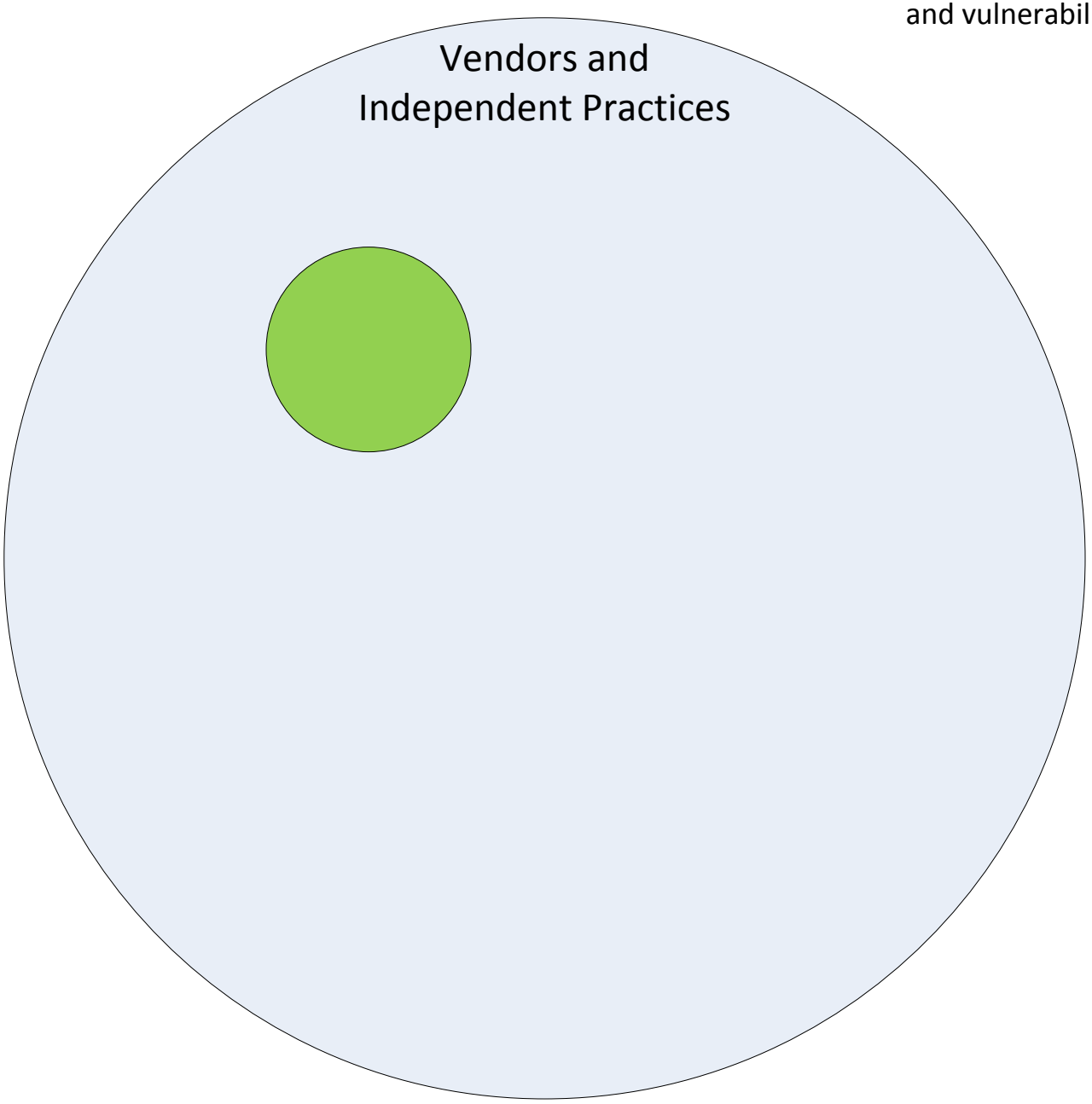
Back to Overview

Colors indicate the level of risk given the current tools, processes and vulnerabilities.



Back to Overview

Colors indicate the level of risk given the current tools, processes and vulnerabilities.



Back to Overview | Back to Parent

Managed Devices - Workstations

Prevention

- Vulnerability Scaning
- Anti-Virus/ Endpoint Protection
- Patching

Detection

Remediation

Containment

- Host Isolation
- Network Isolation

Back to Overview | Back to Parent

Managed Devices - Printers

Prevention	Detection
Remediation	Containment

Back to Overview | Back to Parent

Managed Devices - Scanners

Prevention	Detection
Remediation	Containment

Back to Overview | Back to Parent

Managed Devices - Phones

Prevention	Detection
Remediation	Containment

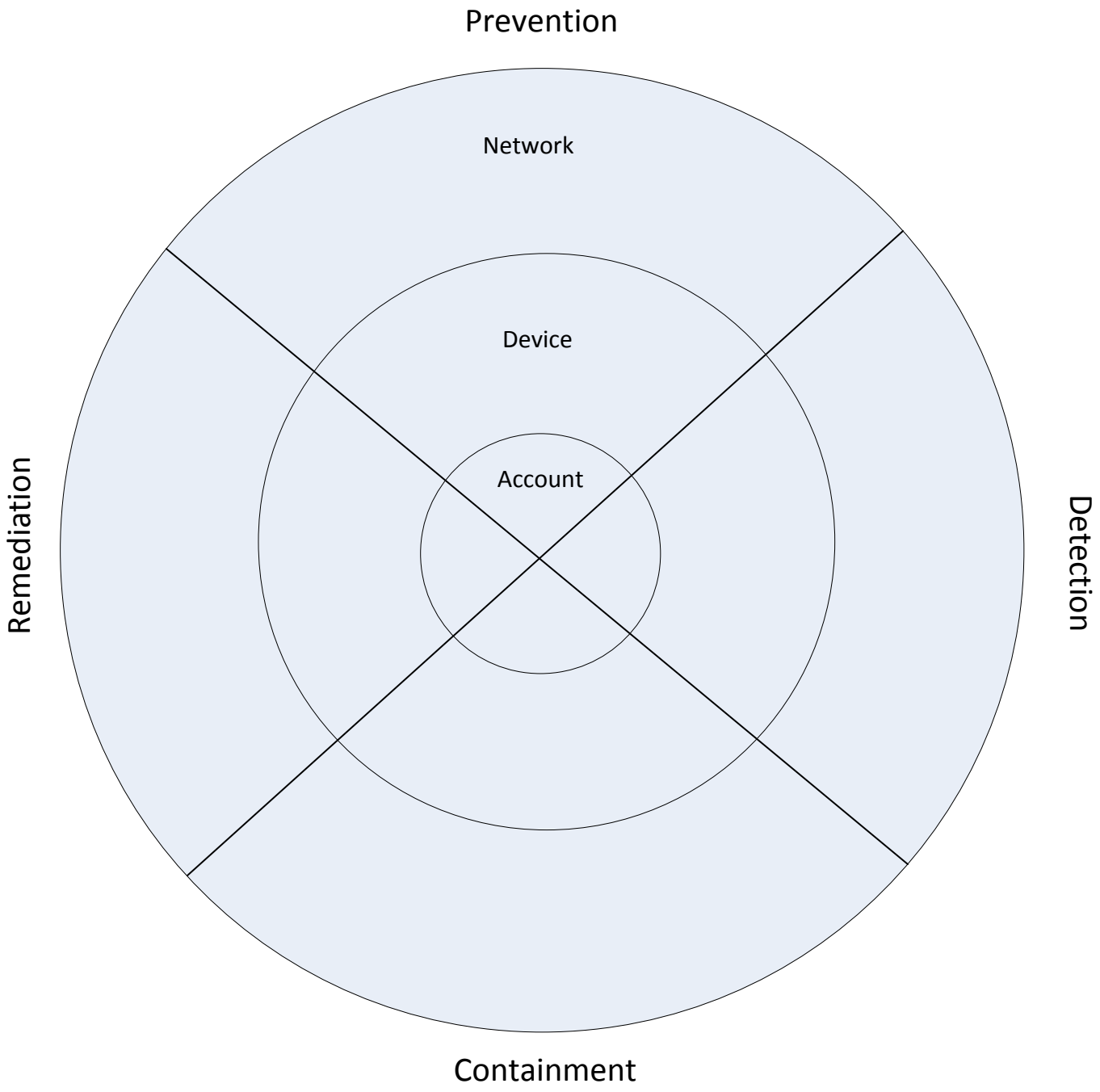
What might Governance or an Auditor want to know in summary about this?

Tools used
Frequency performed
Location for documentation
IT Team responsible

What might Governance or an Auditor want to know in summary about this?

Tools used
Frequency performed
Location for documentation
IT Team responsible

There are four parts to an Information Security program: **Prevention**, **Detection**, **Containment** and **Remediation**. Tools and processes can be applied to different areas within our environment for each of these phases. For example we can prevent malicious programs on a device, when it travels over a network or with settings on an account.



For each phase of Information Security we can either allow what we know to be good (known good) or block what we know to be bad (known bad); each approach has tradeoffs.

If we only block things that are known to be bad we will always be behind the attackers and need to accept more operational risk. When a new attack is discovered a patch will be made, then deployed by the vendor; we will then download the patch, test it and deploy it to our environment. That entire process could take weeks if the patch is tested thoroughly, allowing the attacker time to break in. The alternative is that we cut back on testing to rush the patch but it may result in an unplanned outage if there is an issue with the patch.

If we only allow things that are known to be good we have a lower operational risk and will spend less time chasing down malware; however we need mature internal processes to review and approve technology before it is added to the whitelist of allowed applications. The safest environments use a known good approach, or whitelisting, to remove themselves from a never ending cycle that cannot be won and will only increase in cost over time.