

Requirement 6: Develop and Maintain Secure Systems and Applications



John Elliott

PRIVACY, PAYMENTS, SECURITY AND RISK SPECIALIST

@withoutfire www.withoutfire.com



Requirement 6



Identify vulnerabilities in your estate

Patching

Change control*

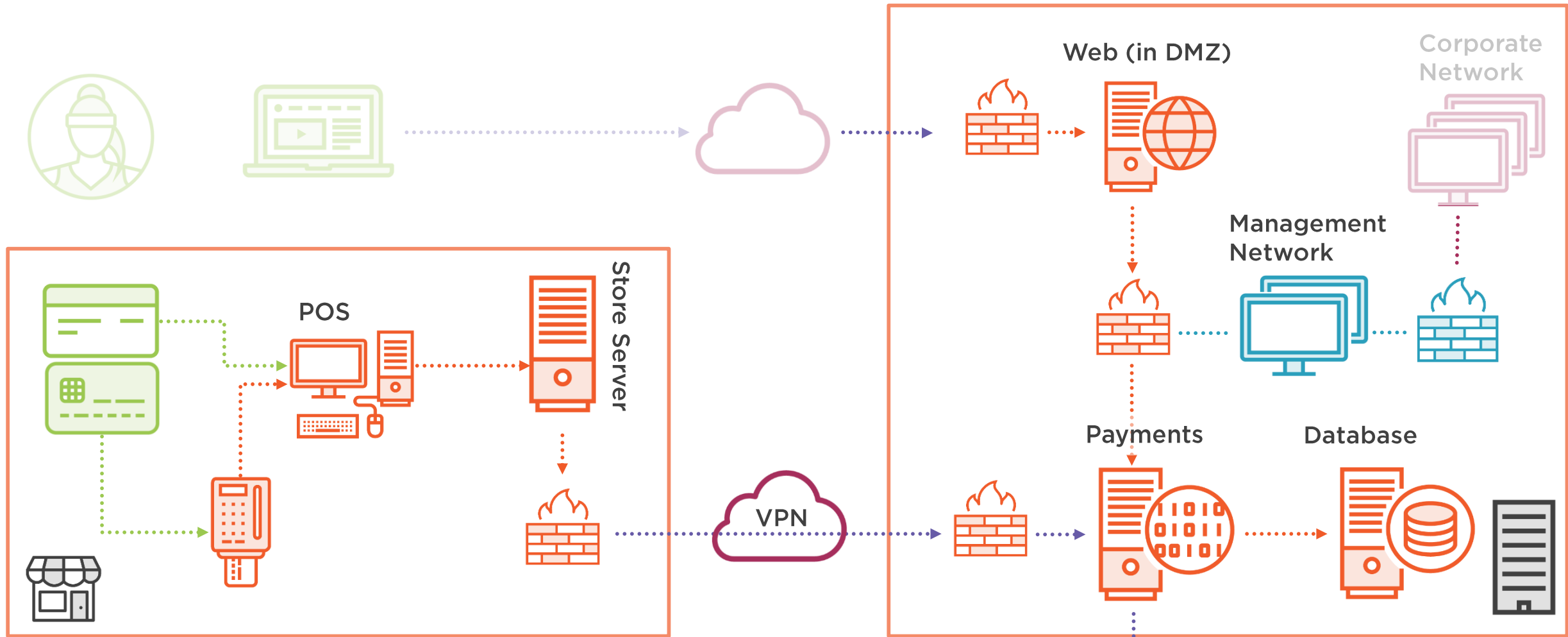
Secure development practices[§]

Secure coding[§]

Protect web-facing applications[§]

Policies and procedures[§]





Vulnerability Management (6.1 6.2)





Requirement 6.1

Identify and risk rank vulnerabilities





Requirement 6.1

Establish a **process** to **identify security vulnerabilities**, using reputable **outside sources** for security vulnerability **information**, and **assign** a **risk ranking** (for example, as *high*, *medium*, or *low*) to **newly** discovered security **vulnerabilities**.



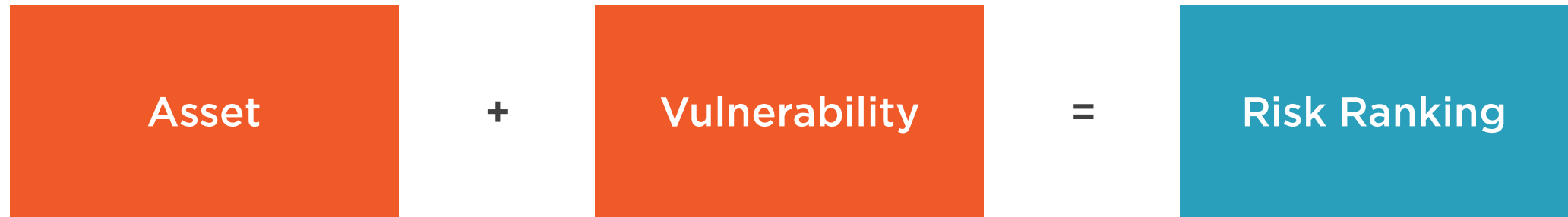
Requirement Guidance

- The intent of this requirement is that organizations keep up to date with new vulnerabilities that may impact their environment.
- Sources for vulnerability information should be **trustworthy** and often include vendor websites, industry news groups, mailing list, or RSS feeds.
- Once an organization identifies a vulnerability that could affect their environment, the risk that the vulnerability poses must be evaluated and ranked. The organization must therefore have a method in place to evaluate vulnerabilities on an ongoing basis and assign risk rankings to those vulnerabilities.

This is not vulnerability
scanning.



Ranking Vulnerabilities



“Poses an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed.”

Critical Vulnerability



6.1 Testing Procedures

Observe/examine systems and settings	!	Agent-based systems
Examine documentation	Y	Policies and procedures
Examine records	!	Previous vulnerability assessments
Interview people	Y	Responsible people





Requirement 6.2

Patch all the things

Patch critical things within one month





Requirement 6.2

Ensure that all system components and software are protected from known vulnerabilities by **installing** applicable **vendor-supplied security patches**. Install critical security patches within one month of release.

***Note:** Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1*



Requirement Guidance

- Prioritizing patches for critical infrastructure ensures that high-priority systems and devices are protected from vulnerabilities as soon as possible after a patch is released. Consider prioritizing patch installations such that security patches for **critical or at-risk systems are installed within 30 days, and other lower-risk patches are installed within 2-3 months**.
- This requirement applies to applicable patches for all installed software, including payment applications (both those that are PA-DSS validated and those that are not).



Please patch critical things
more quickly than this.

(a month is the maximum)

6.2 Testing Procedures

Observe/examine systems and settings	Y	System components
Examine documentation	Y	Policies and procedures
Examine records	!	Change control records, proof of historical activity
Interview people	-	



That's Fine in Theory

