RISK RANKING:

POLICY AND PROCEDURES

INTERNAL USE ONLY

Version Status

This version of this document is currently:

	In Progress
	In Review
	Published
	In Test
⇒	**Tested/Applicable**

Document History

Version	Authors	Reviewers	Publisher	Date	Changes
0.1	Pierre AURE			03/02/2016	Initialization
1.0			Pierre AURE	07/08/2016	Minor update with an update of URI links
1.1		Pierre AURE		03/09/2017	Annual review
1.2		Pierre AURE		05/24/2017	§2.2 chapter "security references" added to the document
1.3		PAU & ATR		01/15/2018	Annual review
1.4		PAU		03/25/2019	Annual review
1.5		PAU		02/24/2020	Annual review
1.6		**ATR**	**PAU**	**03/04/2021**	**Annual review – urls updated**

This Document

Context	This document is part of Accor' response to formalize its vulnerability and patch management process involving the establishment of a Risk Ranking policy.
Contents	This document contains the general rules, responsibilities and process in place in Accor regarding the risk ranking policy.
Audience	This document is addressed to all stakeholders in the Accor IT community, including employees, contractors, interns, and suppliers.
Sources	These policies are based on field experience and industry best practices.
Related Documentation	The set of Security Policies and Procedures documents are currently available from the Accor intranet.
Using this guide	This document presents guidance and principles behind and in procedures, along with general information about procedures. It does not, however, provide an exhaustive user's manual for specific procedures.
Questions?	Contact security@accor.com

Table of Contents

1 Introduction

1.1 Goal

This document defines the process for the establishment of a Risk Ranking policy. It describes the methodology to determine the severity of risk regarding several criteria for Accor environment.

This document is used as a reference guide in the prioritization of tasks for the Patch Management and processes.

1.2 Scope

All components included in the PCI DSS scope must adhere to the rules and process defined in this document.

Other components connected to the Accor Information System may also adhere to the guidelines defined in this document.

1.3 Policy Assumptions

This Risk Ranking policy supplements the *General IT Security Policy* without replacing it or contradicting it. In particular, the present policy shares the following elements from the *General IT Security Policy* document:

- Security principles
- Availability
- Applicability
- Exceptions
- Responsibility
- Penalties
- Policy Reviews
- Related documents

These elements are not repeated in this document.

1.4 PCI DSS requirements related to risk ranking

One requirement in the PCI DSS standard involved risk ranking.

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 newsgroups, 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 achieved by an ASV scan or internal vulnerability scan, rather this requires a process to actively monitor industry sources for vulnerability information.

Classifying the risks allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.

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.

Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.

Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization’s environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. In addition to the risk ranking, vulnerabilities may be considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process or transmit cardholder data.

These requirements are extracted from PCI DSS version 3.2.1 :

PCI_DSS_v3-2-1.pdf

1.5 Overview

The Risk Ranking level definition needs to be reviewed annually taking into account internal and external threats based on field experience and industry best practices.

2 Ranking methodology

2.1 Severity ranking

In accordance with the PCI DSS standard, Accor will adhere to the following definitions regarding severity ranking that are related to all processes within the cardholder environment (CDE).

This severity ranking may also be used for any other IT resources.

Security Threat	Level
• For **components directly reachable from the Internet** ([1]): ○ Vendor patches and security updates defined as "high", "critical" or "urgent" by vendors (except vulnerability that only leads to denial of service) Or: ○ CVSS base score ≥ 4 (except vulnerability that only leads to denial of service) • **All vendor patches that will be evaluated as "Critical" by the Accor Security team**	High
• For **components directly reachable from the Internet** ([1]): ○ Vendor patches and security updates not defined as "high", "critical" or "urgent" by vendors Or: ○ CVSS base score < 4 Or: ○ Vulnerabilities that only lead to denial of service • For all components with an **internal exposure only** • **All vendor patches and security updates for other components**	Low

A justified risk-based analysis or temporary palliative remediation can be supplied by Accor to reduce risk level from High to Low.

[1] Components directly reachable from Internet, also called public-facing devices and systems, are defined in the next paragraph

2.2 Security references

In several processes within PCI DSS, security references are involved as “industry-accepted” and need to be based on (requirements 2.2, 3.4, 3.5.3, 6.5, 9.8, 10.4.3, 11.3).

The following list of references is commonly used by the security community and could be used:

- Hardening guides :
  - Center for Internet Security (CIS) [2]
  - National Institute of Standards Technology (NIST) [3]
  - Editor/vendor documentation
- Encryption and Key Management
  - Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI) [4]
  - National Institute of Standards Technology (NIST) [5]
- Vulnerability
  - Common Vulnerabilities and Exposures [6]
  - Common Vulnerability Scoring System (CVSS) [7] [8]
  - QualysGuard KnowledgeBase [9]

As our vulnerability management tool (QualysGuard VM) correlate several security references, its knowledgebase can be used as a reference database by itself. Several criteria are embedded as:

- CVE ID, Vendor Reference, Bugtraq ID, Patch Availability
- CVSS scoring
- PCI requirement or not (linked to ASV vulnerability classification)

[2] CIS Benchmarks
[3] NIST Special Publications
[4] ANSSI – Cryptographie, les règles du Référentiel Général de Sécurité
[5] NIST – SP 800-57r4, Recommendation for Key Management
[6] Mitre – CVE database and standard
[7] FIRST – CVSS
[8] NIST – CVSS NVD
[9] Qualys – QualysGuard Vulnerability Management

3 Appendix

3.1 Definition

CVSS	*Common Vulnerability Scoring System* A free and open industry standard for assessing the severity of computer system security vulnerabilities
Must	The rule is an absolute requirement
May	The rule is optional

3.2 Related documents

Document name	Purpose
Change Management Process	Change Management Policy and Procedures
Patch management process	Patch Management Policy and Procedures