

BUSINESS



# 网络安全漏洞 管理规范

汇报人：

URS

BUSINESS

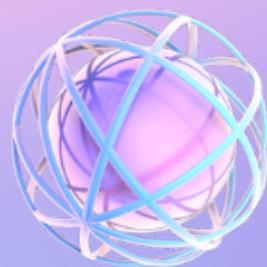


- 1 引言
- 2 网络安全漏洞概述
- 3 网络安全漏洞管理的重要性
- 4 网络安全漏洞管理规范
- 5 具体实施步骤与措施
- 6 网络安全漏洞管理中的技术手段
- 7 网络安全漏洞管理的持续改进
- 8 网络安全漏洞管理的责任与监督
- 9 总结与展望
- 10 结语

# BUSINESS



引言



# 引言

随着网络技术的迅猛发展，网络安全问题已成为社会各界的焦点话题

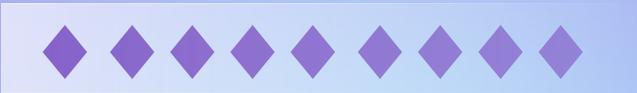


在这个数字化、网络化的时代，如何有效地管理和应对网络安全漏洞，是每个组织和个人都必须认真对待的问题



我将围绕“网络安全漏洞管理规范”这一主题，为大家详细介绍相关内容





# 网络安全漏洞概述



# 引言



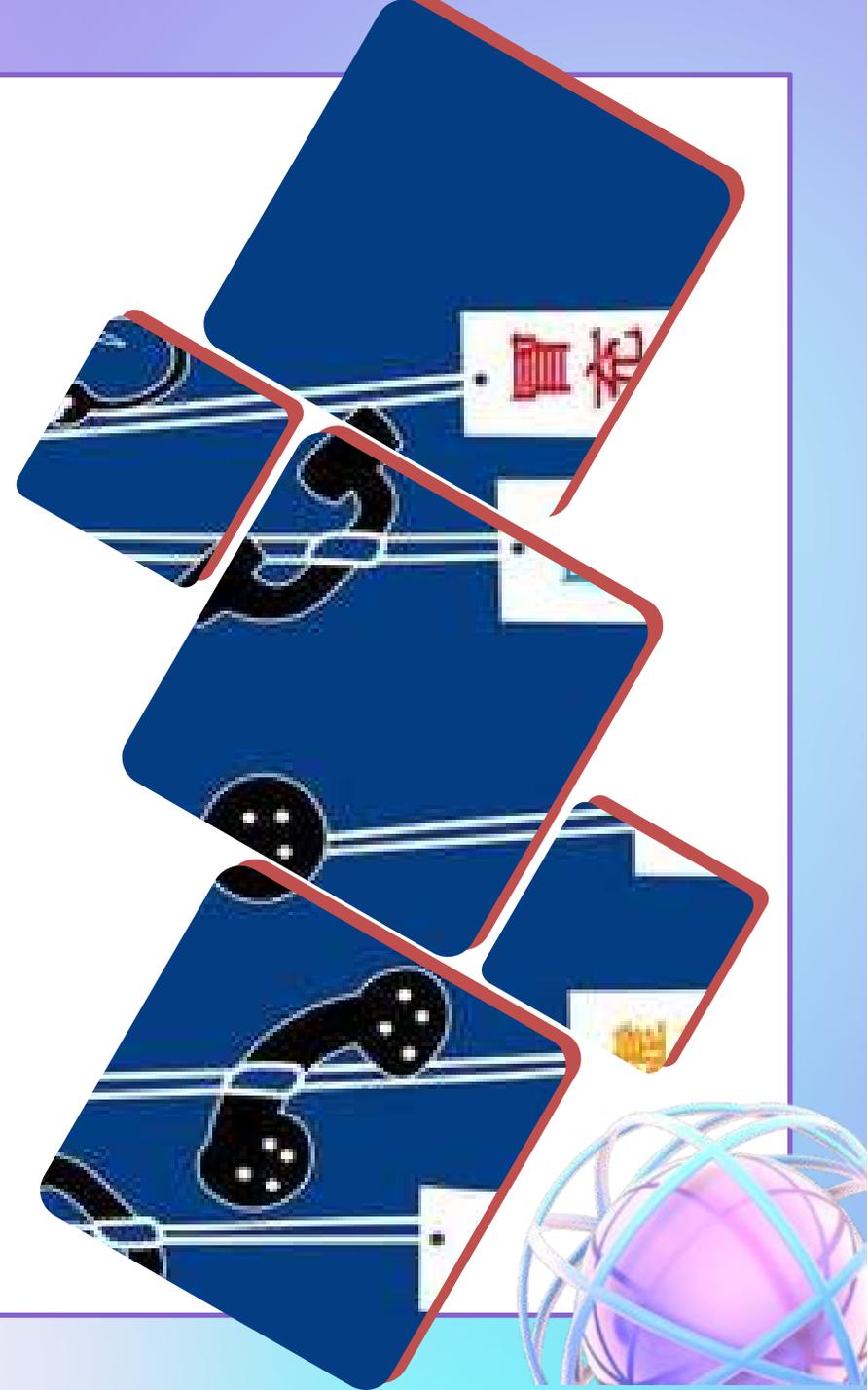
## 1.1 定义与分类

网络安全漏洞是指在网络系统中存在的、可能被恶意利用的缺陷或弱点。这些漏洞包括软件漏洞、硬件缺陷、网络配置错误等。按照影响范围和危害程度，可分为低危漏洞和高危漏洞



## 1.2 漏洞的危害

网络安全漏洞如果不及时修复和防范，可能被黑客利用，导致数据泄露、系统瘫痪、甚至造成严重的经济损失。因此，对网络安全漏洞的管理和防范至关重要



BUSINESS



# 网络安全漏洞管理的重要性



# 网络安全漏洞管理的重要性

## 2.1 保障信息安全

有效的网络安全漏洞管理可以及时发现和修复系统中的安全隐患，保障信息安全，防止数据泄露和系统被攻击

## 2.2 提升系统稳定性

及时发现并处理网络安全漏洞，可以提升系统的稳定性，减少因漏洞导致的系统故障和停机时间

## 2.3 维护企业声誉与形象

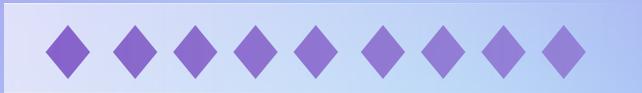
网络安全问题不仅影响企业的经济利益，还可能损害企业的声誉和形象。规范的网络安全漏洞管理，能够提升企业对外形象，增强客户信任



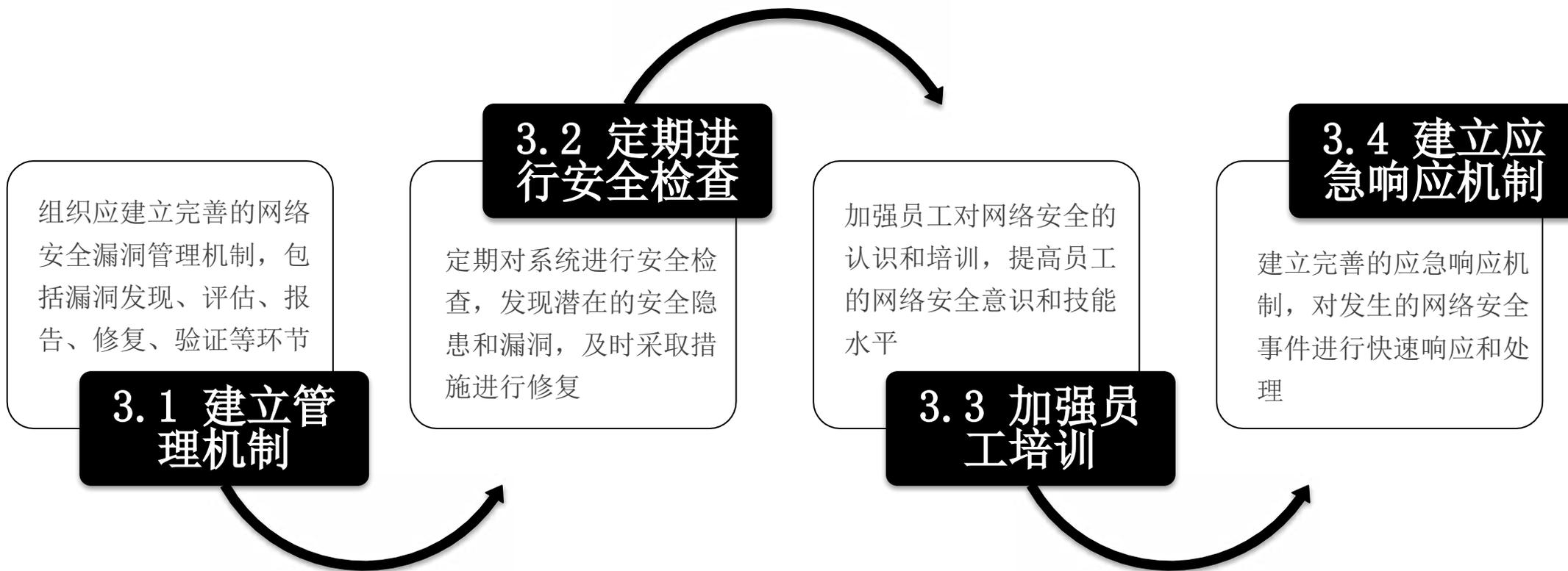
BUSINESS



# 网络安全漏洞管理规范



# 网络安全漏洞管理规范





## 具体实施步骤与措施



以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：  
<https://d.book118.com/328067037064007005>