Separation of development test and production environments

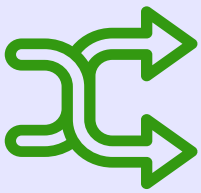
ISO 27002 Control 8.31

Control

Development, testing and production environments should be separated and secured

Purpose

To protect the production environment and data from compromise by development and test activities

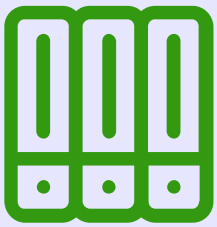


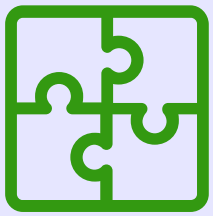
Why is it important?

- Inadequate separation introduces significant risks (e.g., running unauthorized code, data integrity issues) to the production system
- It ensures confidentiality of production information by restricting access for developers/testers
- It enforces segregation of duties by preventing a single person from deploying untested changes directly

What does it imply ?

- Adequately separating development and production systems
- Testing changes to production systems and applications in a testing environment prior to being applied to production systems
- Not making development tools or utility programs accessible from production systems when not required
- Defining roles/segregation of access rights so a single person cannot make changes to both development and production without review/approval





Best practices

- Adequately separating development and production systems
- Defining roles and segregating access rights to prevent one person from making unauthorized changes across environments
- Implementing strong security controls (patching, configuration) on non-production environments

Link with other frameworks

- NIST 800-53 rev5 : CM-4(1), CM-5*, SA-3*
- NIST CSF 2.0 : PR.IR-01

Renaud Dardenne
Asphalia Consulting