Separation of Duties

15 Read it Later

Data Security Regulation & Compliance

The basic principle of separation of duties is that no individual person, role, or group, should be able to execute all parts of a transaction or process. A simple example serves to clarify this principle: a single person should not be judge, jury, and executioner.

In practice, separation of duties is a loss-control measure designed to reduce the risk of accidental or intentional damage to the integrity, confidentiality, and availability of a transaction or process. It serves three primary purposes:

- Reduce the risk of conflict of interest or the appearance of conflict of interest
- Reduce the risk of errors, fraud, abuse, theft, or other wrongful actions.
- Comply with regulatory mandates (e.g., SOX, HIPAA, PCI DSS, GDPR) and industry-specific regulations (e.g., ISO 17799)

A risk-based approach to separation of duties

There is “no one size fits all” plan that organizations can use to ensure separation of duties. Each organization must consider the risks it faces, as well as the compliance mandates it must meet.

Creating a separation of duties plan applicab
conducting a risk-assessment, which involve

1. Conduct data discovery and classification to determine where your sensitive data resides and assess the level of risk to its integrity, confidentiality, and availability.
2. Identify any individual person, role, or group that can:

   Alter, encrypt, or destroy sensitive data, either accidentally or intentionally.

   Exfiltrate sensitive data.

   Influence the design, testing, implementation, and reporting of sensitive data controls.

3. Create a risk map or matrix, based on the results of steps 1 and 2.
4. Implement separation of duties controls, based on the results of step 3. Implementation should use the principle of least privilege necessary to complete a transaction.

What to consider

Although the results of your risk assessment will be unique to your organization, in general, separation of duties controls should ensure that:

Software developers, contractors, and third-party vendors cannot access production systems, database management systems, or system-level technologies.

Functional users and system programmers cannot access or modify source or application code.

End users cannot access or modify production data, except through an appropriate administrative application.

DBAs do not have root or administrator permissions.

Only security system analyst can access system logs and system audits, which is monitored on a regular basis.

Only network security analysts can access firewalls and network security systems, which is monitored on a regular basis.

Only approved operators can make data backup tapes, with regular monitoring to ensure that appropriate compliance p

Only a system security administrator can which are independently monitored on a regular basis for excessive, unauthorized, or unused privileges.

Generic administrator accounts are disabled.

These separation of duties controls create a robust ‘checks and balances’ system that prevents any individual person, role, or group from:

Giving any user account excessive or unauthorized privileges (e.g., permission to

sensitive data).

Modifying sensitive data residing within production systems.

Modifying security systems (e.g., disabling audit functions).

Modifying system logs or audit reports.

See how Imperva Data Security Solutions can help you with separation of duties.

Request demo

Learn more

Practices to facilitate or enforce separation of duties

The following practices are recommended for facilitating or enforcing separation of duties.

Install only approved code on production systems.

Monitor source code repositories for excessive use.

Create unique VLANS for software developers, contractors, and third-party vendors working on any data-related projects.

Create two user accounts for Adminis ut ctivi such as email and one for activities requi permissions.

Use two-factor authentication for privileged users, to ensure the person is who he or she claims to be.

Use network access controls to prevent VLANs from accessing production systems.

Use a write-only logging system administered by a group separate from system and network administrators.

Use role-based access to logging and audit records, to ensure that administrators

cords for their networks or systems.

Use automated tools to manage and audit database access and activities, user rights, and privileged users.

Learn how Imperva solutions can support separation of duties.

Latest Blogs

Data Security

How Imperva Mitigates Security Threats in Oracle Cloud Infrastructures

Bruce Lynch
Oct 25, 2022 4 min read

Industry Perspective •••

Why Cybersecurity Awareness Month is Every Month

7
S
D

Latest Articles

Read it Later

Data Security

SOC 2 Compliance

482.5k Views

Data Security

PCI DSS Certification

139.7k Views

Data Security

Personally Identifiable Information (PII)

96.1k Views

Ir d ir p

84

+1 866 926 4678

Partners

Imperva Partner Ecosystem

Channel Partners

Technology Alliances

Find a Partner

Partner Portal Login

Resources

Imperva Blog

Resource Library

Case Studies

Learning Center

About Us

Who We Are

Events

👋 Hey there! Do you have a minute to chat?

1

Careers

Press & Awards

Contact Information

System Status

Support

Emergency DDoS Protection

Su

Read it Later

Imperva Community

Documentation Portal

API Integration

Trust Center

English

Cookies Settings

Trust Center

Modern Slavery Statement

Privacy

Legal