# Frequently Asked Questions:

[What is IT Segregation of Duties?](#_Q:_What_is)

[Why is my application included in the review?](#_Q:_Why_is)

[Are any Compliance Critical Systems excluded from the SoD Review?](#_Q:_Are_any)

[What is Highly Privileged Access?](#_Q:_What_is_1)

[How do you define Configuration Changes?](#_Q:_How_do)

[How do I remove my application from the review?](#_Q:_How_do_1)

[What if I have a small team and SoD management is not feasible?](#_Q:_What_if)

### Q: What is IT Segregation of Duties (SoD)?

Segregation of duties is a control process that prevents/detects errors or irregularities from being introduced into IT programs. SoD involves reporting all privileged and administrative accounts to verify roles do not provide conflicting privileges or pose a risk.

**Conflicts:** If conflicting access roles are unavoidable, a Security Exception must be requested and a monitoring control must be put into place to periodically validate that no unauthorized changes have been deployed to production.

**Config/UI: *Requirements still being defined by Corporate:*** IT users with access to make configuration changes in non-production environments must not have the ability to implement those changes in production. If users require this access, a process should be established to mitigate the risk (i.e. configuration change windows, configuration change logging and monitoring).

**Database:** Application/Project DBAs may not have update/execute access in the production instance of the database. Update/execute access must be restricted to only those users with valid business reason for requiring access. Only Operations DBAs may have access to both production and non-production instances of the database in order to perform job responsibilities.

**Operating System:** Users may not have access to both production and non-production instances of a server. Users with developer access for the application must not have the ability to deploy changes through production OS backdoor. Users with deployer access for the application must not have access to the application source code through non-production OS backdoor.

### Q: Why is my application included in this review?

All applications were chosen because they are Compliance Critical Systems as defined by the [GE Corporate System Classification Standard](http://libraries.ge.com/download?fileid=378751726101&entity_id=27315898101&sid=101):

Availability Impact = High or Severe (the impact on the GE Company of a system outage.) **Or**,

The application is a part of a critical physical or logical security system **Or,**

Application contains, processes, transmits or stores:

Sensitive data

* + - PII (employee/contractor, consumer, medical, personal bank accounts, cards, SSN or Gov ID’s, special data)
    - Government data (classified, controlled unclassified)
    - 3rd Party Organizational Data
    - Export license required data from any country

System Integrity information

* + - SOX
    - Non-SOX financial data
    - Payment Card Industry – controlled data
    - Product quality
    - Physical or logical security

### Q: Are any Compliance Critical Systems excluded from SOD reviews?

Applications whose source code is not developed or maintained within GE, are considered Out of Scope for SOD review. For example, a third party vendor develops and maintains the application/product-based application.

Notify PMO team via email if your application as not applicable.

### Q: What is Highly Privileged Access?

Access that provides:

* Ability to change master data (i.e. customers, vendors, products, prices…) that impact business functions and/or global definitions
* System Administrator abilities (e.g. root for Unix/Linux, windows administrator, database administrator, access to all data)
* Ability to create/modify/delete users (may be application specific)
* Override of application controls that the business relies on
* Change configurable parameters
* Ability to make direct changes in database (does not include changes made through the application)

Management accounts - Accounts that come with the product and are used to manage the database (e.g. sys, system)

Monitoring accounts - Accounts used to monitor the database (normally comes with product installation)

Schema Ancillary Accounts – Accounts that are used to manage the schemas in a database instance.

Any additional accounts identified by the asset owner that are considered privileged

All non-personal highly privileged accounts (External users (vendors/suppliers/customers having access to a database)

### Q: How do you define Configuration Changes?

Configuration can refer to:

* Hardware
* Software
* A combination of hardware and software
* System component set up
* The assortment of components that make up the system

When installing new devices, you may need to set various switches and jumpers (for hardware) and define values of parameters (for software). Thanks to new technologies, such as plug-and-play, much of this configuration is performed automatically. In some cases System have privileges for managing configuration changes.

### Q: How do I remove my application from this review since it is not a critical application?

Use the [Compliance Impact Assessment workflow](http://supportcentral.ge.com/ProcessMaps/form_new_request.asp?prod_id=63877&form_id=574572&node_id=1925876&map_id=&reference_id=&reference_type=) to submit a request to change the critical system flags for your application

### Q: What if I have a small team and SoD management is not feasible?

If you have a small team where members perform multiple functions resulting in conflicting privileges, then please submit an [Aviation IT Risk Acceptance and Security Exception](http://supportcentral.ge.com/ProcessMaps/form_new_request.asp?prod_id=63877&form_id=525743&node_id=1691113&map_id=&reference_id=&reference_type=) workflow request.

Once completed, share the exception document to the PMO team for documentation purposes.