Deloitte.

Security of Information Systems within European Institutions
Define IT Security Plans in line with Commision's Decision 3602

Information Security planning and compliance challenges

In today's complex economic and political environment, the European Institutions heavily rely on information systems to achieve their strategic goals and missions, and to effectively implement their annual work programmes. It is a fact that Information Systems developed and managed by European Institutions are more complex and interconnected then ever. They are also expected to be "best in class" examples of security, reliability and resilience.

Aware of these needs, the European Commission issued the Decision C(2006) – 3602 on security of information systems. The Commission's Decision 3602 and the related Standards and Guidelines provide for security measures for the protection of the involved information systems and the information processed therein against threats to their availability, integrity and confidentiality.
The Decision 3602 applies to all Directorates-General and departments in all places of work, including the Joint Research Centre and the delegations in third countries, offices linked administratively to the Commission and all Executive Agencies or other bodies using the Commission's information systems.

To comply with the requirements of Decision 3602, the responsible stakeholders must elaborate an IT Security Plan (ITSP) for all information systems – ITSPs should be based on a proper Business Impact Assessment (BIA) and Risk Analysis (RA) to ensure sufficient and appropriate security measures are in place.

Framework for achieving compliance with Commission's Decision 3602 and the related Standards and Guidelines

1. Preparation & info gathering	• Define the scope of IT Security Plans • Obtain understanding of the information systems in scope • Inform and involve key business and IT stakeholders
2. Assets identification	• Compile and update the asset inventory for the information system • Validate the asset inventory
3. Business impact assessment	• Conduct business impact assessement workshops with the business and IT officers • Validate the business impact assessement and report
4. Security classification	• Perform security classification of information system, in line with European Commission guidance • Finalize security classification with business and IT
5. Risk analysis	• Perform the risk analysis in line with European Commission guidance • Validate the risk analysis and report
6. Prepare the IT Security Plan (ITSP)	• Draft IT Security Plan • Validation workshop of the ITSP (with business, IT, LISO, SSO, etc.) • Validate and publish the ITSP
7. Establish monitoring process for ITSPs implementation	• Define overall monitoring process for the ITSPs implementation progress and status • Define dashboard for monitoring ITSPs implementation progress and status • Define a roadmap for the monitoring actions

Your benefits

We will directly work for you in order to ensure compliance with the main requirement of Commission's Decision 3602 that all information systems shall have a documented IT Security Plan.
Additionally our specialized professional services will help:

- Align the IT security efforts and priorities with the annual work programme and with the strategic goals of the DG/Agency;
- Support directly the role and compliance obligations of:
  - Heads of IT or Business Units (HoU) responsible for the Information Systems (IS)
  - Local Information Security Officers (LISO)
  - System Security Officers (SSO)
  - Project Managers (PM)
- Increase the transparency of the security and compliance efforts from both IT and business units with regards to the Information Systems (IS) they manage;
- Minimize the internal efforts from your unit/team to plan and apply cost effective security measures based on business risk exposure of the involved Information Systems and assets;
- Use the achievement of compliance with Commission's Decision 3602 to prepare and provide the documentary evidence for compliance with other information security related standards and frameworks that are relevant for the European Institutions (e.g. ISO 27001, COBIT, ENISA, NIST, etc.);
- Establish a process to ensure continuous monitoring of the security compliance for involved Information Systems with the requirements of the Commission's Decision 3602 and the related Standards and Guidelines.

Framework contracts that can be immediately used for delivery of these services to the DGs of the European Commission

We are happy to inform you that there are two applicable framework contracts that can be used for delivery of these services – in order to immediately provide support for the Heads of Unit (HoU), Local Information Security Officers (LISO), System Security Officers (SSO) and Project Managers (PM) in their efforts for ensuring compliance with existing EC 3602 Standards and Guidelines.

Framework contract DESIS III Lot 4 (30CE06694230009)

The framework contract DESIS III Lot 4 "Off-site developments, studies and support" is already in place and can cover services related to assistance to elaborate IT Security Plans in line with the requirements of EC 3602 Standards and Guidelines.

Deloitte Senior Consultants (SC) and Consultants (CO) with specific information security and EC 3602 Standards and Guidelines can immediately and directly assist you by preparing the IT Security Plans at your convenience, either:

- On-site (intra-muros) or off-site (extra-muros)
- In a time and means (TM), quoted time and means (QTM) or in a fixed price (FP) mode

This framework contract is supported by DG DIGIT and covers all European Commissions Directorates and Services. In addition to the European Commission itself, the resulting contract will apply to the following awarding authorities, all of which are Executive Agencies located in Brussels or Luxembourg:

- EACEA
- EAHC
- ERC EA
- INEA (ex-TEN T EA)
- REA

Framework contract STISS III Lot4 (DI/07057-00)

Furthermore, the framework contract STISS III Lot4 "Information Solutions engineering, development, testing and support" is also already in place and can cover services related to assistance to elaborate IT Security Plans in line with the requirements of EC 3602 Standards and Guidelines.

Deloitte Technology Experts can immediately and directly assist you by preparing the IT Security Plans at your convenience, either:

- On-site (intra-muros) or off-site (extra-muros)
- In a time and material or in a fixed price mode

This framework contract is supported by DG DIGIT and covers all Commissions Directorates and Services.

For further information, please contact:

Dan Cimpean
+ 32 497 59 38 27
dcimpean@deloitte.com

Nicolas Courtin
+ 32 2 749 57 36
ncourtin@deloitte.com

Ahmed Maaloul
+ 32 473 45 01 75
ahmaaloul@deloitte.com

3436