management procedure shall involve ICT security to assess potential impact of the change on the risk level related to IT Contractors' remote access.

ECHA shall continuously monitor threats and risks, and perform annual risk assessments. In case of a significant change in the risk profile a process to update security rules and requirements and adding additional mitigation factors is activated.

4.2. ECHA's operational roles and responsibilities

The role of ICT Security Officer is to support the implementation of the policy and to advise the Director of Information Systems for what pertains to the application of this policy.

Framework Contract Managers are responsible for the governance of security whenever applicable to the framework contracts they are responsible for.

Contract Managers, Service Managers and other persons who have a key role in IT service outsourcing shall be aware of this policy and related security model. They are responsible for making sure that this policy and related security model are applied whenever remote access is granted.

ECHA's operational roles and related tasks to apply the policy are listed in more detail in the table below.

Role	Tasks
New IT Contractors' Access	
Director of Information Systems	• Make a decisions based on the ICT security officer's advice
FWC Manager	• Communication with the IT Contractor • Contract amendments • Set up security governance model with the IT Contractor • Represent ECHA in the security governance
Contract Manager (Specific contracts)	• Ensuring the application of the policy and the security model are followed whenever remote access has to be granted
ICT Security Officer	• Defining which access level category the requested access belongs to (if not the default access level (Highest)) • Checking if specific risk assessment is needed • Performing specific risk assessment if needed • Evaluation of the equivalency of potential compensating controls • Compliance checking based on the documentation delivered by IT Contractor (Ch. 5.2 below) • Assessment of sufficiency of IT Contractor's practices to check and evaluate security measures and controls, and report results to ECHA (Ch. 5.3 below) • Make proposals to the Director of Information Systems based on the assessments
Management of the existing IT Contractor's access	
Director of Information Systems	• Supervising and providing required resources • Steering in the security governance