

European Commission selects Capgemini for its EU cybersecurity framework contract



[Capgemini](#) today announced that it has been selected by the [European Commission's Directorate-General for Digital Services \(DIGIT\)](#) to provide comprehensive cybersecurity services to public institutions across the European Union, as part of a consortium with Airbus Protect, PwC, and NVISO. The MC17 FREIA Cyber Framework Contract is a multi-million Euro agreement spanning four years. As part of this, Capgemini will help strengthen cybersecurity capabilities and protect critical digital infrastructure across 71 European Institutions, Bodies, and Agencies (IBAs).

The consortium was selected for all three lots, reflecting its combined strength in delivering across the entire cybersecurity value chain. Together with the other consortium partners, Capgemini will play a key role in supporting Europe's cyber resilience and digital sovereignty, focusing on areas such as operations and incident response, governance and risk management, and training and technical expertise.

The approach will support NIS2 Directive[\[1\]](#), the Digital Operational Resilience Act (DORA), the EU Cybersecurity Act, and the Cyber Resilience Act. These services will help EU institutions enhance resilience, address evolving cyber threats, and drive long-term digital transformation.

Bringing together complementary strengths, the consortium will mobilize the full breadth of Capgemini's cybersecurity expertise, to deliver end-to-end support from strategy to execution.

“The awarding of all three lots to our consortium underscores the European Commission’s trust in our capability to deliver complex cybersecurity programs at scale,” said Marc Reinhardt, Global Public Sector Leader at Capgemini. “It reflects not only our technical expertise but also our commitment to supporting Europe’s vision of digital sovereignty and institutional resilience. By combining strategic foresight with operational agility, we will help European institutions address today’s threats and prepare for tomorrow’s challenges.”

[1] <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>