France

Your local contact

Valérie Aumage
Partner, PwC Legal France
+33 6 60 75 02 84
valerie.aumage@avocats.pwc.com

Nolwenn Vignaud
Senior Manager, PwC Legal France
+ 33 7 63 80 21 48
nolwenn.vignaud@avocats.pwc.com

Status	Draft
Name of National Law	Bill on the resilience of critical infrastructures and the strengthening of cybersecurity
Entered into force	Expected Q3 of 2025
Link to current draft or equivalent	https://www.assemblee-nationale.fr/dyn/17/textes/l17b1112_projet-loi.pdf
Scope (deviating from NIS-2-Directive)	**Material Scope**: Other critical sectors include research in addition to NIS-2 Annex II. Additional entities in scope. Most important deviation is that essential entities include entities from a highly critical sector which employ at least 250 individuals **OR** which have a turnover of more than 50 million euros **and** an annual balance sheet of more than 43 million euros. **Territorial Scope**: The general criterion is that the entity is subject to French law if it is established in France. For certain digital infrastructure entities, for ICT service management and for digital providers, French law applies if the entity has its main establishment in France.
Registration	Important and Essential entities must register with the French National Cybersecurity Agency (ANSSI) through a web portal https://monespacenis2.cyber.gouv.fr/ (not live yet). The ANSSI must ensure that the list is updated at least every 2 years.
Information Security Standards referenced	No reference to international security standards is included in the Bill. The Bill however specifies that a referential of technical and organisational measures will be published for essential and important entities, which could include obligations to use products, services or processes which are certified by the ENISA under EU Regulation 2019/881.
Incident reporting	Significant incidents must be reported to the ANSSI according to the following timeline (from discovery of the incident): • Within 24 hours: initial report; • Within 72 hours: intermediate report (for trust service providers, this report must be sent within 24 hours) • Within 1 month after the intermediate report: final report or, to the extent the incident has not been dealt with, a status report which shall be completed by a final report within 1 month after the incident has been dealt with.
Authority / CSIRT	French National Cybersecurity Agency (ANSSI)
Fines (deviating from NIS-2-Directive)	Sanctions are pronounced by a special sanctions commission. • Sanctions applying to essential entities cannot exceed EUR 10.000.000 or 2% of the annual worldwide turnover, excluding taxes. • Sanctions applying to important entities cannot exceed EUR 7.000.000 or 1.4% of the annual worldwide turnover, excluding taxes.
Worth mentioning	The draft bill is not expected to change much. However, additional terms will be specified by decree (including the subsectors which are considered as highly critical or critical, the cybersecurity measures which must be implemented by covered entities and the list of information to be provided when registering as a covered entity). Fines and incidents can be made public.