During 2015, the Research Center of Cyber Intelligence and Information Security (CIS) of the University of Rome Sapienza (http://www.cis.uniroma1.it/en) and the Cyber Security National Laboratory of National Interuniversity Consortium for Informatics (https://www.consorzio-cini.it/lab-cyber-security) started to work on a National Framework for the Cyber Security.

The outcome, Italian National Framework for the Cybersecurity (ITF), is compliant to the Framework for Improving Critical Infrastructure Cybersecurity (CSF) in order to favor International harmonization.
ITF has been tailored according to the Italian market context with a specific focus on small and medium enterprises. The ITF derives from the NIST Framework the basics of Framework Core, Profile and Implementation Tier.

According to the Italian market landscape, we found extremely useful to introduce three important concepts in the CSF.

* Priority levels. The priority levels define which is the priority associated to every single Subcategory of the Framework Core. It should be noted that every organization is free to adapt its own priority levels according to type of business, size and own risk profile.

* Maturity levels. The maturity levels define the various extent to which every single Subcategory of the Framework Core can be implemented. The selected maturity level is to be carefully evaluated by each single enterprise according to its business and size, as well as its risk profile. Typically, higher maturity levels require greater effort both in financial and management terms. For some Subcategories it is not possible to establish maturity levels.

* Framework contextualization. Creating a contextualization of the Framework (for a productive sector, for business type or a single business), means to select the Function, Category and Subcategory of the relevant Framework Cores, specifying the priority and maturity levels appropriate for the implementation context.

The framework contextualization is particular important, since it allows to give to the Framework a greater generality defining specific vertical frameworks on market sectors.

The Italian National Framework for the Cybersecurity (that is attached in pdf) also provides an example of contextualization, designed for Small and Medium Enterprises (SMEs) that is business sector independent.

Other contextualizations could be done specifically by trade associations and regulatory bodies, so that they are acknowledged by an entire production sector or by a regulated sector. As far as regulated sectors goes, in some cases the implementation priorities of some security controls at a basic maturity level could become compulsory according to sector regulations.
Link to the
document: http://www.cybersecurityframework.it/sites/default/files/CSR2015_ENG.pdf