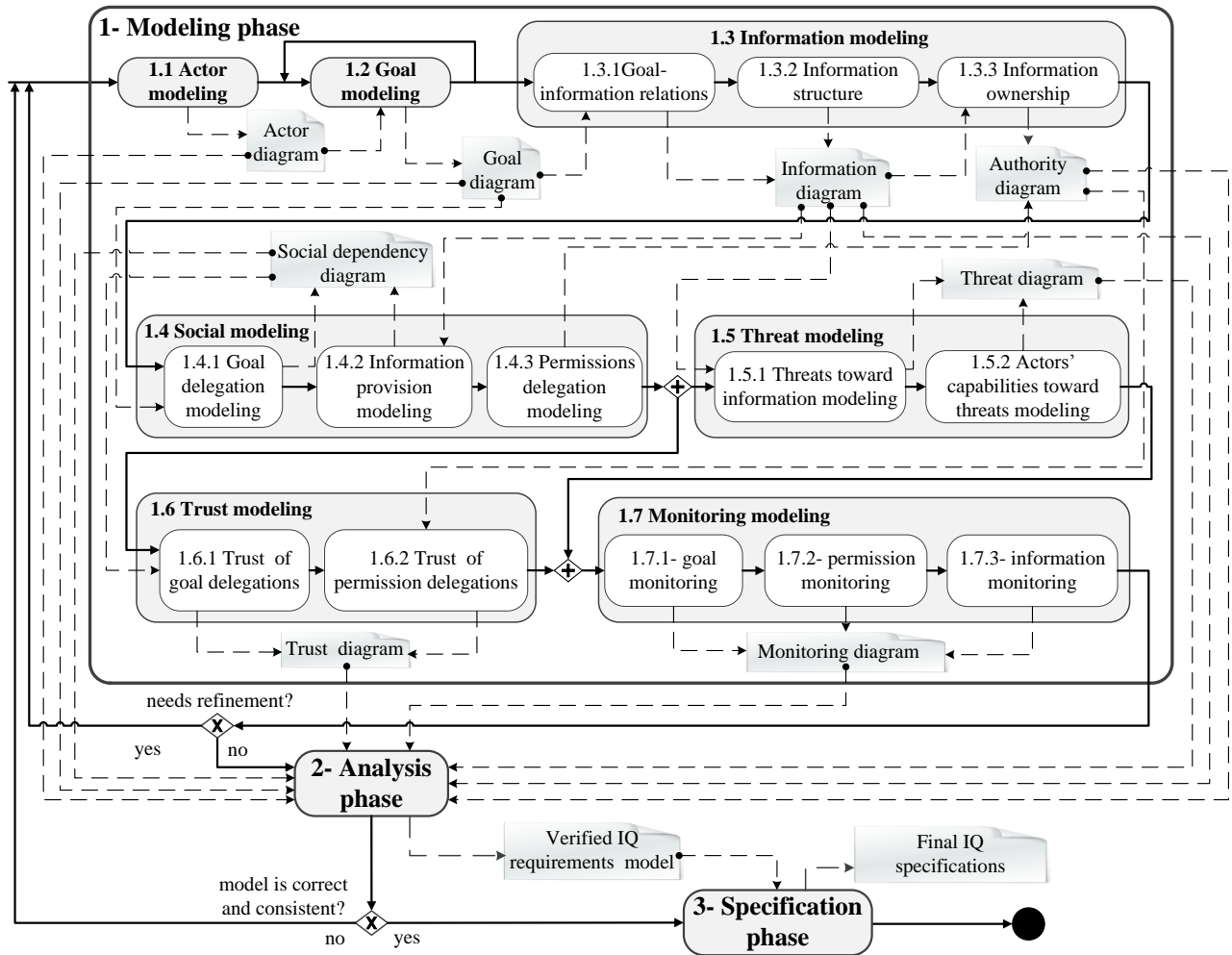


# The Methodological Process

The process (depicted in Figure 1) aims to support system designers during the overall system design process, and it is composed of three main phases:



**Figure 1 Methodological process for modeling and analyzing IQ Requirements**

**1. Modeling phase:** aims to model the system-to-be through seven sequential modeling activities:

**1.1 Actor modeling:** is the first modeling activity that aims to identify the *actors* of the system in terms of *agents* and *roles* they are playing along with their capabilities. The outcome of the actor modeling activity is the *actor diagram* that is used as an input for the *goal modeling* activity.

**1.2 Goal modeling:** aims to model actors' objectives in terms of goals, and refine these goals through and/or decompositions until reaching their leaf sub-goals that are fine enough to be achieved by actors. Goal modeling is an iterative activity, i.e., it might be repeated several times. The outcome of this activity is the *goal diagram* that is used as an input for both 1.3.1 *goal-information relations* and 1.4.1 *goal delegation* activities.

**1.3 Information modeling:** aims to model *information* along with its different relations with other modeling constructs. This activity is composed of three sub-activities: 1.3.1 *Goal-information relations* that models the different relations between goals and information (e.g., produce, read, modify and send), and it takes the *goal diagram* as an input; 1.3.2 *Information structure modeling* that models the relations between information and its sub-parts; 1.3.3 *Information ownership modeling* takes the *information diagram* as an input, and models the relations between owners and information they own. The outcome of the first two activities (1.3.1 and 1.3.2) is the *information diagram*, while the outcome of the last (1.3.3) is the *authority diagram*.

**1.4 Social modeling:** aims to model the different social relations among the actors of the system concerning the transfer of their entitlements and authorities, where this activity is composed of three sub-activities: 1.4.1 *Goal delegation modeling* that takes the *goal diagram* as an input, and models goal delegations among the actors; 1.4.2 *Information provision modeling* that takes the *information diagram* as an input, and models information transmission among the actors; 1.4.3 *Permission delegation modeling* that models the delegation of permissions among actors. The outcome of the first two activities (1.4.1 and 1.4.2) is the *social dependency diagram*, while the outcome of the last activity (1.4.3) is used to update the *authority diagram*.

**1.5 Threat modeling:** aims to model information related threats along with actors' capabilities toward them, and it is composed of two sub-activities: 1.5.1 *threats toward information modeling* that take the *information diagram* as an input, and models threats that might threaten information; 1.5.2 *Actors' capabilities toward threats modeling* models actors' capability/incapability toward each identified threat, where the outcome of these two activities is the *threat diagram*.

**1.6 Trust modeling:** aims to model trust relations among the actors concerning their social dependencies, and it is composed of two sub-activities: 1.6.1 *Trust of goal delegations* that takes the *social dependency diagram* as an input, and model trust/distrust relation among actors concerning their delegated goal; and 1.6.2 *Trust of permissions delegations* that takes the *authority diagram* as an input, and model trust/distrust relation among actors concerning their delegated permissions. The outcome of these two activities is the *trust diagram*.

**1.7 Monitoring modeling:** aims to model the different monitoring relations among the actors concerning their different dependencies. This activity is composed of three sub-activities: 1.7.1 *Goal monitoring* models goal monitoring relations among the actors, i.e., when an actor does not trust another one for achieving a delegated goal, a monitoring relation is required. 1.7.2 *Permission monitoring* models permissions monitoring among the actors. 1.7.3 *Information monitoring* aims to model information monitoring among the actors concerning the provided information. The outcome of these three activities is the *monitoring diagram*.

**2- Analysis phase:** aims to verify the correctness and consistency of the IQ requirements model. In particular, the analysis phase takes the IQ requirements model in terms of its different diagrams (e.g., actor, goal information, etc.), and perform the required analysis to verify its correctness and consistency against the properties of the design, i.e., the model is correct and consistent, if all of these properties hold. After the analysis activities are completed, and if there are inconsistencies and/or conflicts in the IQ requirements model, the process starts again from the modeling phase to refine the model accordingly. Otherwise, the process proceeds to the final phase of the process (*Specification phase*). The outcome of this phase is a verified IQ requirements model.

**3- Specification phase:** aims to automatically derive the final IQ specifications in terms of IQ policies from a verified IQ requirements model. The analysis and specification phases are automated activities, and they are fully supported by the STS-IQ Tool.