Modeling Cyber Systemic Risk for the Business Continuity Plan of a Bank

Angelo Furfaro, Teresa Gallo, Domenico Saccà

Modeling cyber systemic risk for the business continuity plan of a Bank

Angelo Furfaro, Teresa Gallo, and Domenico Saccà

University of Calabria - P. Bucci, 41 - 87036 Rende (CS) – Italy
{a.furfaro, t.gallo, sacca}@dimes.unical.it

Abstract. The pervasive growth and diffusion of complex IT systems, which handle critical business aspects of today's enterprises and which cooperate through computer networks, has given rise to a significant expansion of the exposure surface towards cyber security threats. A threat, affecting a given IT system, may cause a ripple effect on the other interconnected systems often with unpredictable consequences. This type of exposition, known as cyber systemic risk, is a very important concern especially for the international banking system and it needs to be suitably taken into account during the requirement analysis of a bank IT system. This paper proposes the application of a goal-oriented methodology (GOReM), during the requirements specification phase, in order to consider adequate provisions for prevention and reaction to cyber systemic risk in banking systems. In particular, the context of the Italian banking system is considered as a case study.

Keywords: Business Continuity, Disaster Recovery, Systemic Risk, Cyber Threat, Goal-Oriented Methodology, Requirements Engineering

1 Introduction

During the last few years, the diffusion of cyber threats has seen a steep growth at a rate which is predicted to increase in the near future [13]. Cyber security threats include events such as accidental cyber-related incidents or deliberate actions coming from external entities such as hacker attacks and virus/worm/malicious software infiltrations [17]. These threats might directly affect industrial control systems and processes and need to be properly managed [22]. The effects of a threat exploit on a given system, may propagate through communication networks causing damages to other interconnected systems and giving rise to a ripple effect. This phenomenon, where a threat triggers a knock-on effect among different enterprises, is known as *systemic risk* and has been the subject of many studies in the financial and economic domains [16].

Provisions against the cyber systemic risk are usually directed to establish a strategy for circumscribing negative effects, e.g. by activating alternative solutions to the damaged systems, and to slow down, and possibly to stop the propagation towards the other interconnected systems.

Nowadays, a big-enterprise IT system is usually geographically distributed, pervasive and ubiquitous for its internal and external users. Therefore, each of such systems consists of a network of subsystems where the cyber systemic risk must be reduced as much as possible. Cyber security risk has to be continuously monitored, while real-time recovery and support procedures, assuring an enough degree of system availability, have to be provided [1,4]. Systemic effects have to be reduced and global collaboration among all stakeholders, both public and private, should be provided for an effective proactive prevention of a cyber shock of our global, not only financial, networked systems [21].

In a recent white paper [5], the Depository Trust & Clearing Corporation (DTCC) affirms that a global cyber systemic risk could become less dangerous if the defense is both collective and coordinated, otherwise the failure is quite sure. The last DTCC report on systemic risk [14] is very alarming on the cyber risk for the worldwide financial markets. Therefore, instead of providing specific cyber risk defenses for each system, a global cyber systemic risk [26,27] strategy should be devised and enforced by means of the adoption of shared rules, regulations and common approaches.

This paper focus on the banking context and, specifically on the business continuous plan (BCP) and its disaster recovery plan (DRP), as regulated by the Bank of Italy for the banking operators located in Italy [6]. However, each Bank operating in the European Union must provide similar guidelines for BCP and DRP of their banking operators.

The definitions of BCP and DRP are driven worldwide by many sectoral rules and regulations [25], without any global coordination. A supervising institution, having the authority to push and actually drive the different BCPs, would be able to manage the global systemic risk by a coordinated strategy. Moreover, the 2016 edition of "The Global Risks Report" [11], by the World Economic Forum, outlines the need for cooperation among stakeholders for risk management and cites some tests performed in Germany.

We model, by means of a goal oriented methodology [23] named GOReM [18], the requirements for the cyber systemic risk treatment for a bank operating in Italy. All Italian banks follow rules and regulations delivered by the Bank of Italy. However, each European Nation has a central banking institution which establish similar guidelines for the local banks. Then, the developed models might be applied, with small adaptations, to whichever bank in Europe.

In particular, the models obtained using GOReM, follow what established by Bank of Italy in the guidelines [6]. Those models allowed to easily highlight how a BCP has two different ways to handle the cyber systemic risk. The first includes critical processes which might develop contagion only to the internal stakeholders of the bank (including counterparts cooperating to the business of the bank). In this case the ripple effect of an incident is treated at the bank level and the Bank of Italy is only notified. The second cyber systemic risk treatment is related to the safeguard of systematically important processes of the payment systems and of the access to financial markets. In this case, both BCP and the handling of a possible ripple effect of an incident on other banks and, more

generally, on external entities, is strongly centralized by the Bank of Italy. The latter is a hierarchical control, although with rigid response time, which might introduce delays in the tentative to slow down or stop contagion in the European and even worldwide financial system [16].

GOReM has already been successfully employed in the context of some industrial research projects, involving enterprises such as ACI Informatica [7] and Poste Italiane [10]. The numerous GOReM practical models in different contexts, including that of system security compliance in cloud [19], allowed to improve the methodology potentialities and to achieve a very good satisfaction of the many stakeholders, which are different in backgrounds and for desired goals.

The rest of the paper is structured as follows: Section 2 describes an overview of GOReM; the requirements specification of a Cyber Systemic Risk in Bank is presented in Section 3. Finally, results and conclusions are drawn in Section 4.

2 An overview of GOReM

This description of GOReM is a small overview which we use often with the aim to give a mean to understand the models hereafter introduced. GOReM uses the UML notation [9]. As a consequence, it is easy to employ and it simplifies the concept sharing among a wide variety of stakeholders [15]. The resulting requirements modeling activity has been recognized by the users to be easy and effective. Typical activities of requirements engineering (RE) [23], i.e. elicitation of requirements, analysis, validation, verification and management, are expressed in GOReM mainly in term of: (i) stakeholders and their goals, (ii) use cases and involved processes and (iii) work-product documentations. The methodology consists of three main phases, each of which is devoted to modeling specific aspects of a RE process: Context Modeling, Scenario Modeling and Application Modeling (see Fig. 1).

Context Modeling aims at clearly representing the reference domain. The work-products of this phase are: a *Stakeholder Diagram*, which shows a, often hierarchical, specification of all the stakeholders involved in the specific context; each stakeholder is in turn characterized by a set of *Softgoals* [20] they intend to pursue; a *Softgoal Dependency Diagram*, which shows the relationships between the stakeholders and the softgoals, as well as the relationships among softgoals (i.e., contributes, hinders, includes, extends, specializes); moreover, the *Rules and Regulations* that govern the context are individuated and analyzed in a work-product.

Scenario Modeling specifies different business scenarios in terms of *Roles* that are played by the involved stakeholders, their specific *Goals*, and the specific *Rules and Regulations* that govern the business scenario. A *SWOT* Analysis (Strengths, Weaknesses, Opportunities and Threats) is often performed with the aim to guide decisions on future work.

Application Modeling defines application scenarios in order to specify the functionalities which should be provided by a single business scenario resulting from the previous phase. Each application scenario is characterized by

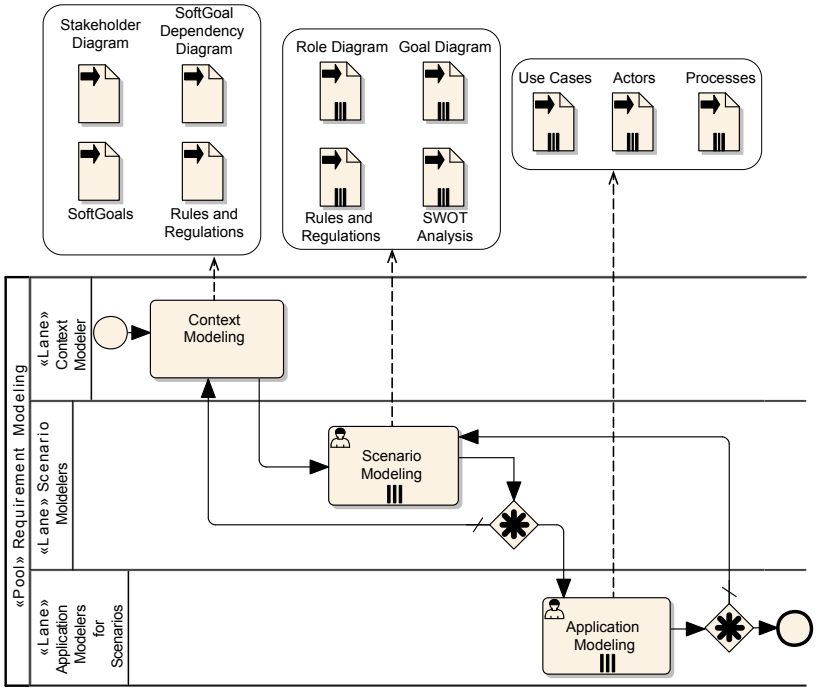

Fig. 1. Reference Process Model of GOReM and Work Products

functionalities that are modeled by UML-based *Use Cases*, *Actors* and possibly *Processes*.

These phases are repeated iteratively and feedback among them is allowed in order to support an incremental refinement process. Furthermore, scenarios and applications are specified concurrently. A BPM model [3] of the reference process for GOReM, along with its main work-products, is reported in Fig. 1.

3 Modeling the banking cyber systemic risk

This Section describes a comprehensive subset of the requirements specification of the business continuity for Italian banks, as established by Bank of Italy in its guidelines in [6], as it has been worked out, employing GOReM, in the context of the project [10].

The context model of the business continuity in a bank and the description of one of the possible business scenarios, that is the risk treatment in bank, are first described. Then, one specific application scenario, concerning the treatment of cyber systemic risk for the so called "systematically important processes" [6] of a bank, is modeled in terms of actors, use cases and processes.

3.1 The Context Model: banking business continuity

The banking system has a complex organizational infrastructure. In the following, we model a small subset with the only objective to give an idea of the effectiveness and powerfulness of employing GOReM for this purpose.

The term *Business Continuity* (BC) refers to all of the organizational, technical and staffing measures employed in order to: (i) ensure the continuation of core business activities in the immediate aftermath of a crisis and (ii) gradually ensure the continued operation of all business activities in the event of sustained and severe disruption [2].

To this end, each bank must define a Business Continuity Plan (BCP), i.e. a formal document stating the principles, setting the objectives, describing the procedures and identifying the resources for business continuity management concerning critical and systemically important corporate process [6]. The bank must also use internal audit, testing activity and continuously improvement implementations of its BCP, with the aim to: (i) analyze well the exposure to risks, (ii) identify vulnerabilities, and (iii) evaluate, implement and maintain updated, appropriate BC and Disaster Recovery (DR) solutions. A critical part of the BCP is the Disaster Recovery Plan (DRP), i.e. a document establishing the technical and organizational measures to cope with events that put electronic data processing (EDP) centers out of service.

Despite suitable tools and countermeasures are constantly in action to prevent their occurrence, unfortunately accidents happen. In this cases, it is essential that a BCP is promptly put in operation, to ensure the continuity of services. Hence, the appropriated Disaster Recovery procedures, as specified by the DRP, have to begin immediately.

Fig. 2 shows a GOReM diagram that depicts the stakeholders which were identified for this context, their softgoals and the dependencies among them.

The main stakeholders are: the **Bank of Italy**; **Banking System Operator**, which can be of two different types, i.e. **Operator of technological infrastructures or networks**, and **operating companies**, i.e. wholesale markets in government securities, multilateral wholesale trading facilities in government securities, multilateral deposit trading systems, securities settlement systems, central counterparties and central securities depositories, with registered offices and/or operational headquarters in Italy; **Bank personnel**, i.e. people, including corporate bodies, which work internally in the bank; **Service Provider**, i.e. external stakeholders that provide IT services and other commodities, by stipulating specific contracts with the bank; **Selling Net**; **Shareholder** and **Customer**.

Each stakeholder is associated to a set of softgoals as it can be seen from Fig. 2. The identified softgoals are resumed in the following.

SG1: Supervising the non-interruption of the bank's services.

SG2: Every operator has to put into execution the suitable provisions, according to the BCP, for ensuring business continuity and disaster recovery in reaction to threats.

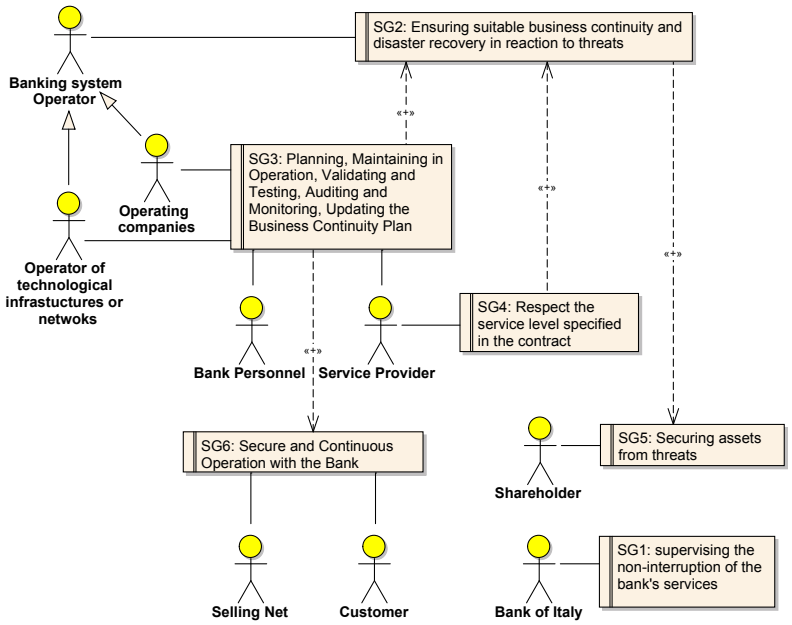

Fig. 2. Context Model: The Banking Business Continuity's Softgoals and Dependencies Diagram

SG3: Planning, keeping into operation, validating and testing, auditing and monitoring, updating the BCP. This softgoal is shared by all kinds of considered bank operators.
SG4: Guaranteeing the service level specified in the contract (i.e. external providers must stipulate a contract with the bank that specifies a service level agreement among the parties and that has to be compliant to the business continuity needs).
SG5: Safeguarding assets from threats. Shareholders need to be ensured about the safety of their financial assets.
SG6: Guaranteeing secure and continuous operation of the bank. Both customers and selling nets need always working and safe banking services.

Fig. 2 also outlines the existing dependencies among Softgoals. In particular, the achievement of SG3 and SG4 contributes to SG2. Similarly, reaching SG2 has a positive effect on SG5 and analogously the same holds for SG3 on SG6.

3.2 Scenario Model: Risk treatment

The scenario we choose to model is about the treatment of risks coming from bank defaults, financial and market crashes, human mistakes, cyber threats and so on. This scenario includes situations such as: destruction or inaccessibility of important structures, unavailability of critical information systems, unavailability of human resources essential to corporate processes, interruption of operation

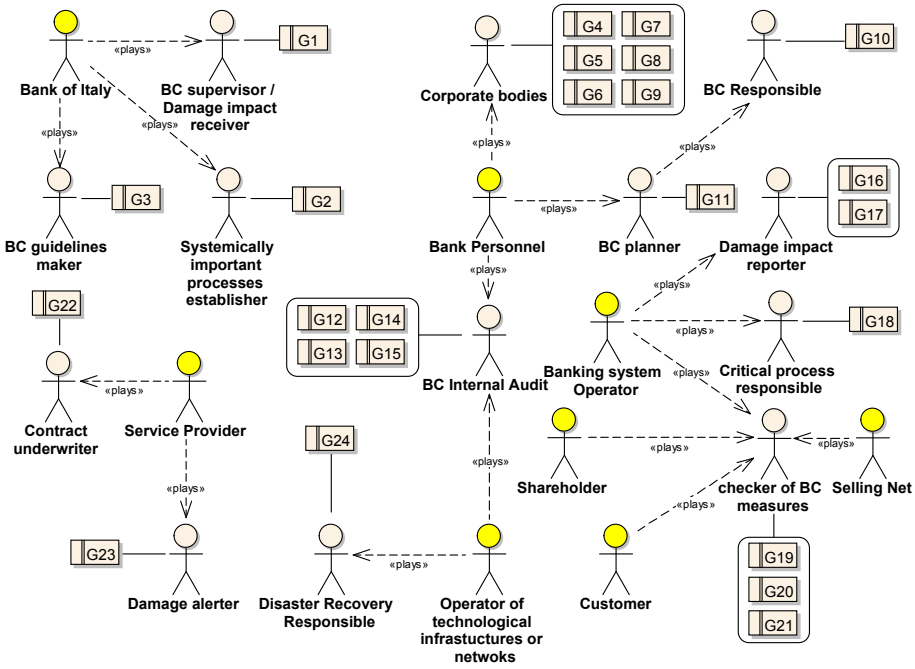

Fig. 3. Scenario Model for Risk treatment: SoftGoals-Roles-Goals Diagram

of infrastructure (e.g. electricity, telecommunications, interbank networks, financial markets), alteration or loss of critical data and documents.

According to the Bank of Italy guidelines [6], operators must define, monitor, test and maintain updated, a BCP for coping with the above situations of crisis involving the operators or significant counterparts as, other group members, major suppliers, prime customers, specific financial markets, clearing, settlement and guarantee systems.

An important step in applying GOReM is the identification of the roles played by each involved stakeholder. Each Stakeholder, while playing a given role, has some specific goals he want to reach inside the scenario. The stakeholders-roles mapping alongside the role-specific goals are resumed by the diagram reported in Fig. 3.

Table 1 details each goal of the considered scenario while Table 2 lists a subset of the rules and regulations of interest for the scenario of Risk treatment. A unique identifier is associated to each rule/regulation and some relationships of warning with respect to others rules/regulations is given (column W) for indicating the need of a deeper analysis when applied in practice.

Table 1. Scenario model for Risk treatment: Role and Goal Description

Stakeholder	Role	Goal	Description
Bank of Italy	BC supervisor / Damage impact receiver	G1	Each operator has its suitable Business Continuity Plan and the impact of possible damages undergone by its Banks for specific systemically important processes, is managed
	Systemically important processes establisher	G2	Systematically important processes are individuated and assigned for being protected by a suitable operator
	BC guidelines maker	G3	Each operator refers to guidelines for business continuity aligned with the actual European level of risk knowledge
Bank personnel	Corporate bodies, i.e. considered part of the bank personnel	G4	Establish objectives and strategies for BCP of the bank
		G5	Assign human, technological and financial resources sufficient to attain the objectives of the BCP
		G6	Approve the BCP and successive modifications resulting from technological and organizational adjustments and formally accept the residual risks not covered by the BCP
		G7	Control the results of checks on the adequacy of the BCP and of its measures, done at least once a year
		G8	Designate the person responsible for business continuity planning
		G9	Promote the development and regular checking of the BCP and its adaptation to any significant organizational, technological or infrastructural innovations and in the case of detection of shortcomings or the materialization of new risks
	BC Responsible	G10	Supervise the planning of the BCPs by means of the coordination of every involved BC planner
	BC Planner	G11	Establish the BCP for the operator, compliant to the guidelines provided by Bank of Italy
	BC Internal Audit	G12	Check, at fixed times, the BCP and its updating by examining the test programs, taking part in the tests and checking the results, and suggesting changes to the BCP on the basis of the shortcomings found
		G13	Analyze the criteria for escalation in the case of incidents, by evaluating the length of time required to declare the state of crisis
		G14	Test the BCPs of the outsourcers and other critical suppliers and may decide to rely on the controls performed by the structures of the latter if they are deemed professionally capable, independent and transparent
		G15	Examine the outsourcing contracts to make sure that the level of safeguards conforms the corporate objectives and standards
Banking System Operator	Damage Impact reported	G16	Produce an impact analysis, preliminary to the drafting of the BCP and regularly update the impact analysis, with the aim to determine the level of risk for each corporate process and highlight the repercussions of a service outage. The impact analysis considers, in addition to operational risks, also such other risks as market and liquidity risk
		G17	Document the residual risks, not handled by the BCP, which must be explicitly accepted by the competent corporate bodies
	Critical process responsible	G18	Identify relevant processes relating to corporate functions whose non-availability, owing to the high impact of the resulting damage, necessitates high levels of business continuity to be achieved through preventive measures and BC solutions activated in case of incident
	Checker of BC measures	G19	Shareholders, together with the bank system operators and the selling net , as well as with customers, cooperate in defining the procedures for testing the planned business continuity measures in real crisis scenarios
		G20	Determine an appropriate frequency of the testing task for each measures
		G21	Write down and notify the results of tests to the competent corporate bodies and transmit, for the matters under their respective competence, to the operational units
Service provider	Contract underwriter	G22	Ensure the service levels agreed with the operators, as formally state in the signed contract, in the case of crisis and ensure the continuity provisions to be put in place in keeping with attainment of corporate objectives and with the indications of the Bank of Italy
	Damage alerter	G23	Notify promptly the operator of any incident, in order to allow immediate activation of the BC procedures
Operator of technological infrastructures or networks	Disaster Recovery Responsible	G24	Define and maintain updated the DRP, with reference to central and peripheral information systems

Table 2. Scenario model for Risk treatment: Rules and Regulations Diagram

Id	Rules and Regulations	Type	Location/ Adopter	W
A	CPMI-IOSCO consultative paper "Guidance on cyber resilience for financial market infrastructure", November 2015	Best practice	EU	B, C
B	Opinion of the European Central Bank of 25 July 2014 on a proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (CON/2014/58)	Policy	EU	A, C
D	Guidelines on business continuity for market infrastructures	Best practice	Italy	A,B, E, F
E	Legislative Decree 385/1993 (the Consolidated Law on Banking)	Law	Italy	A, B, G
F	Legislative Decree 58/1998 (the Consolidated Law on Finance)	Law	Italy	A, B, H
G	Business continuity oversight expectations for systemically important payment systems, issued by Eurosystem in June 2006	Best practice	European Union	E, F, H
H	Principles for Financial Market Infrastructures, issued by Bank for International Settlements Committee on Payment and Settlement Systems (CPSS) and IOSCO Technical Committee, April 2012	Best practice	European Union	E, F, G

3.3 Application Model: Cyber Systemic Risk for banks in Italy

The application model we consider is related to the Cyber Systemic Risk as dealt with by the Bank of Italy. This is one of the application models that might be derived from the above presented Risk Treatment scenario.

This application model deals with business continuity and safeguards for the so referred "Systematically Important Processes", which are identified and controlled directly by the Bank of Italy and which govern essential services in the payment system and in the access to the financial markets. A malicious exploitation of a cyber threat for these processes might evolve in a systemic crisis inside other operators and on the whole financial system. For those processes, the Bank of Italy controls, asks for updates, and manages every risk of crisis and incidents.

The Bank of Italy requires that the operators, involved in systematically important processes, work actively for adjustment of the BCP. These operators must comply with stricter business continuity requirements than those which normally apply to all operators. In particular, these requirements are concerned with the recovery time of systemically important processes, the location of standby facilities, and the resources allocated to crisis management (see section III of [6]).

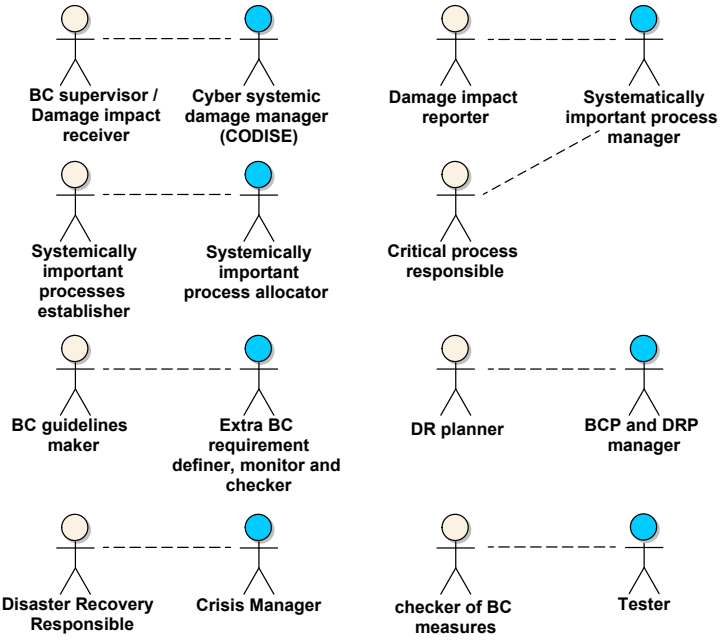

Fig. 4. Application Model for Cyber Systemic Risk: Actor Diagram

Fig. 4 shows the Actors Diagram relevant to this application model, where scenario roles are mapped to actors, and Fig. 5 resumes the main use cases involving the identified actors.

Some use cases are extensions of some others which are supposed to be already defined in another application model, named "Business continuity management", where the constraints by the Bank of Italy are less stringent and related to critical processes which are not systematically important processes. A short description of these use cases is given below.

BCP adjustments and compliance monitoring (**eUCa**). This use case extends the use case **UCa** which is part of the use cases concerning critical processes which do not belong to the set of those considered *systematically important*. BC and DR plans, defined in the application model "Business Continuity Management", require some adjustments to become compliant with the stricter requirements defined by the Bank of Italy. The operator must also ensure continuous compliance with the special requirements and all this must be done by the responsible for these activities (i.e. the actor "BC and DR plans requirement adjustment and compliance responsible").

Main incidents and recurrent criticality check (**eUCc**). This use case extends the use case **UCc** (*Business continuity plan checking*). The Bank of Italy requires at least one a year of test for the safeguards provided for the continuity of the systemically important processes. Operators must actively participate in tests

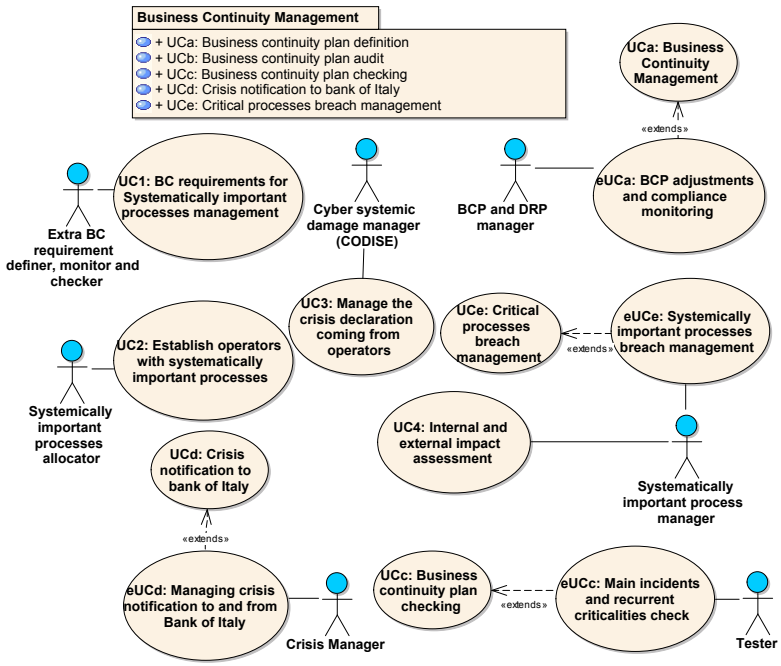

Fig. 5. Application Model for Cyber Systemic Risk: Main Use Case Diagram

and market-wide simulations, organized or promoted by authorities, by markets and by the main financial infrastructures. In addition, this use case prescribes the drafting of a yearly report about: the main features of the business continuity plan; the adaptations that have been made to it; the additions implemented during the year; the tests conducted on the main incidents and criticalities.

Managing crisis notification to and from Bank of Italy (**eUCd**). This use case extends the use case **UCd**, related to notification to Bank of Italy, when the blockage of essential infrastructures is related to internal critical processes. In this case, the actor "crisis manager" must instead communicates promptly to the Bank of Italy every cyber attack and state of crisis coming from some threat to its systemically important processes. Furthermore, the use case includes the sending of an assessment report, drafted according to **UC4**. In addition, this use case dictates that the "crisis manager" receives the notification, coming from the Bank of Italy, that other operators are subject to a cyber attack, which might cause contagion to some of its systematically important processes. Then, this actor should raise an alert so that recovery procedures may immediately begin (see **UC3**).

Systemically important processes breach management (**eUCe**). This use case extends the use case **UCe**. The actor "systemically important processes manager" activates immediately the recovery procedures as indicated by the BCP

and DRP when a breach to some process under its observation occurs. As specified by the guidelines, these procedures govern:

(i) the recovery time that, if the cause of the blockage is internal to the operator, must not exceed four hours and the restart time must not exceed two hours. If the blockage is due to an external contagion, the operator must activate his DR within two hours from the restart of the first affected operator. For information systems with on line duplication of operational data the time between the recovery point and the incident should zeroed. In case of extreme situations, promptly recovery of systemically important processes, using protected off line PCs, faxes, and telephone contacts with selected counterparts, is allowed.
(ii) the location of standby facilities, which must be distant from their primary facilities, possibly outside the metropolitan area in which the primary facility is located and it must be served by utilities (i.e. telecommunications, electricity, water) different from those serving the primary facility.
(iii) the resources allocated to crisis management. Human, technological and logistical resources needed to keep systemically important processes operating are established in the BCP.

BC requirements the management of systematically important processes (**UC1**). Stricter BC requirements for systematically important processes are established by Bank of Italy. This use case directly controls the operators adjustment and the compliance of their BCPs to the evolving requirements imposed by the Bank of Italy.

Establish which operator has systematically important processes (**UC2**). The Bank of Italy is in charge to individuate the specific set of operators having systematically important processes.

Manage the crisis declaration coming from operators (**UC3**). For incidents that may have significant impact on systemically important processes, the declaration of the state of crisis is managed by CODISE, part of Bank of Italy, which begins this activity with an initial assessment of potentially damaged operators.

Internal and external impact assessment (**UC4**). In the occurrence of crisis, the actor "systematically important processes manager", prepares the assessment of the impact on operations of its central and peripheral structures and of the current relations with customers and counterparts.

Fig 6 and Fig. 7 report two activity diagrams that respectively model the process of handling cyber systemic risk for important banking processes and the process of managing the possible know-on effect of a cyber systemic incident inside the important processes of an operator.

4 Results and Conclusions

We tested the suitability of GOReM for modeling the context of business continuity in of a Bank and the requirements related to handling of the cyber systemic risk as regulated by the guidelines issued by the Bank of Italy. In the complex and

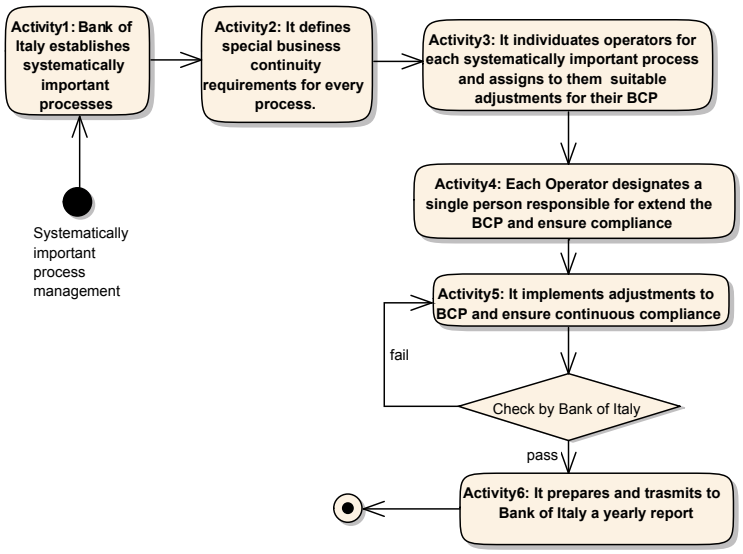

Fig. 6. Application Model for Cyber Systemic Risk: Sistemically important processes Management Process

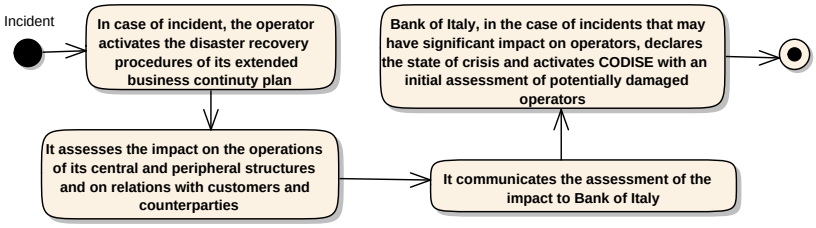

Fig. 7. Application Model for Cyber Systemic Risk: Incident Management Process

touchy scenario of banking, the relevant models have been defined and graphically represented [15]. GOReM allowed to easily identify stakeholders, roles and specific goals from which the main use cases and processes, have been derived. The result of this study is a requirements specification that may be employed as a good starting point for the devising a global approach towards the management of the cyber systemic risk in the financial and banking domain. In fact, it gives the adequate planning independence to the single bank, but under the riverbed of the constraints dictated by a supervisor authority, like the Bank of Italy for the Italian banking operators. Moreover, this vision could scale at the behavior of a node inside a bigger network, where other nodes are the other Bank of the other European Nations. In turn, this model might be applied to a coordinated European supervision institution, e.g. the European Systemic Risk Board [12]. Even more, it is also desirable to scale worldwide under the control of a global

authority, which might coordinate business continuity and disaster recovery for preventing and managing a cyber systemic risk, for the global financial world.

As a final consideration, special attention should be paid to the time needed for a given operator to react to a cyber incident: be "promptly" might not be an adequate answer. Two observations come from this modeling experience:

(i) Cyber systemic effects are here handled by a central authority, which in this case is the Bank of Italy, that establishes the state of crisis and manages the know-on effect on other operators. This centralization may result in a waste of time even though prudential politics suggest that this is a good strategy.
(ii) Time of response to a state of crisis that is communicated after some "hours" (see use case **eUCe**) might be a very large interval of time, especially at a worldwide level, compared to the speed of cyber threats.

A possible solution might be in modifying the hierarchical organization in a more horizontal and collaborative one, which might come only from common decided rules and regulations [8]. However, Cyber Systemic Risk treatment in Europe and worldwide is nowadays urgent. According to [24], while business areas are already supervised, the supervision agreement for network and information security is still a work in progress. This is a big delay for cyber systemic risk that must be regained soon.

5 Acknowledgments

This work has been partially supported by the "National Operative Programme for Research and Competitiveness" 2007-2013, Technological District on Cyber Security (PON03PE_00032_2_02), funded by the Italian Ministry of Education, University and Research, and the Italian Ministry of Economic Development.

References

1. Business continuity oversight expectations for systemically important payment systems (SIPS). Report, Eurpean Central Bank (2006), https://www.ecb.europa.eu/pub/pdf/other/businesscontinuitysips2006en.pdf
2. Escb definitions of major business continuity terms in relation to payment and securities settlement systems. , European Central Bank (Jun 2007)
3. Business Process Model and Notation^{TM} v. 2.0. Spec. formal/2011-01-03, Object Management Group (2011), http://www.omg.org/spec/BPMN/2.0/
4. Principles for financial market infrastructures. Press release ISBN 92-9197-108-1, Bank for International Settlements Committee on Payment and Settlement Systems (CPSS) and IOSCO Technical Committee (2012)
5. Cyber Risk a Global Systemic Threat: A White Paper to the Industry on Systemic Risk. White paper, Depository Trust & Clearing Corporation (DTCC) (October 2014), http://www.dtcc.com/%7e/media/Files/Downloads/issues/risk/cyber-risk.pdf
6. Guidelines on business continuity for market infrastructure. guidelines, Bank of Italy (2014), https://www.bancaditalia.it/compiti/sispaga-mercati/codise/Guidelines_business_continuity_market_infrastructures.pdf

7. DICET-INMOTO - ORganization of Cultural HEritage for Smart Tourism and Real-time Accessibility (OR.C.HE.S.T.R.A.) - Project funded by the Italian Ministry of Education, University and Research (MIUR) - PON Project - Research and Competitiveness 2007-2013 (2015)
8. Market intermediary business continuity and recovery planning. Tech. Rep. FR32/2015, International Organization of Securities Commissions (December 2015), http://www.iosco.org/library/pubdocs/pdf/IOSCOPD523.pdf
9. Unified Modeling Language^{TM}, v. 2.5. Spec. formal/15-03-01, Object Management Group (2015), http://www.omg.org/spec/UML/2.5/
10. District of cyber security (2016), https://www.distrettocybersecurity.it
11. The global risks report 2016. Insight report, 11th edition, World Economic Forum (2016), http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf
12. Handbook on the assessment of compliance with ESRB recommendations. European Systemic Risk Board (2016)
13. Internet Security Threat Report. Volume 21, Symantec (Apr 2016)
14. Systemic risk barometer: Results overview 2016 - Q1. Press release, Depository Trust & Clearing Corporation (DTCC) (2016), http://www.dtcc.com/%7E/media/Files/PDFs/Systemic-Risk-Barometer-Q1-2016.pdf
15. Caire, P., Genon, N., Heymans, P., Moody, D.L.: Visual notation design 2.0: Towards user comprehensible requirements engineering notations. In: 21st IEEE International Requirements Engineering Conference (RE 2013). pp. 115–124. Rio de Janeiro, Brasil (July 2013)
16. Cerutti, E., Claessens, S., McGuire, P.: Systemic risks in global banking: What available data can tell us and what more data are needed? Working Paper 18531, National Bureau of Economic Research (November 2012), http://www.nber.org/papers/w18531
17. Chaudhary, R., Hamilton, J.: The five critical attributes of effective cybersecurity risk management - white paper. Tech. rep., Crowe Horwath LLP (2015)
18. Citrigno, S., Furfaro, A., Gallo, T., Garro, A., Graziano, S., Saccà, D.: Mastering concept exploration in large industrial research projects. In: INCOSE Italia Conference on Systems Engineering (CIISE 2014). pp. 26–37. Rome, Italy (November 24-25 2014)
19. Furfaro, A., Gallo, T., Garro, A., Saccà, D., Tundis, A.: Requirements specification of a cloud service for cyber security compliance analysis. In: Proc. of the 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech'16). IEEE, Marrakesh, Morocco (May 24–26 2016)
20. Glinz, M.: On non-functional requirements. In: 15th IEEE International Requirements Engineering Conference (RE 2007). pp. 21–26. IEEE, New Delhi, India (October 2007)
21. Goldsmith, D., Siegel, M.: Systematic approaches to cyber insecurity. Tech. rep., MIT Sloan School of Management1 - ECIR Working Paper (2012)
22. Kosub, T.: Components and challenges of integrated cyber risk management. Zeitschrift für die gesamte Versicherungswissenschaft 104(5), 615–634 (2015)
23. van Lamsweerde, A.: Goal-oriented requirements enginering: a roundtrip from research to practice [enginering read engineering]. In: 12th IEEE International Requirements Engineering Conference. pp. 4–7. Kyoto, Japan (September 2004)
24. Nouy, D.: Single supervisory mechanism after one year: the state of play and the challenges ahead. In: Bank of Italy Conference on Micro and macroprudential banking supervision in the euro area. Milan, Italy (24 November 2015), https://www.bankingsupervision.europa.eu/press/speeches/date/2015/html/se151124.en.html

25. Rissman, D.: US regulators issue guidance on disaster recovery and business continuity planning for hedge funds (2013), http://aceits.net/us-regulators-issue-guidance-on-disaster-recovery-and-business-continuity-planning-for-hedge-funds/
26. Sommer, P.: Reducing systemic cybersecurity risk. Oecd/ifp project on future global shocks, Information Systems and Innovation Group, London School of Economics and Ian Brown, Oxford Internet Institute, Oxford University (2011), https://www.oecd.org/gov/risk/46889922.pdf
27. Tendulkar, R.: Cyber-crime, securities markets and systemic risk. Joint staff working paper, IOSCO Research Department and World Federation of Exchanges (2013), http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf