A Framework for Project Risk Assessment in Telehealth

Emilio Sulis
Computer Science Department
University of Turin
Turin, Italy
ORCID: 0000-0003-1746-3733

Alex Cordero
Computer Science Department
University of Turin
Turin, Italy
alex.cordero@unito.it

Simone Donetti
Computer Science Department
University of Turin
Turin, Italy
simone.donetti@unito.it

Paolo Ferrero
Augeos S.p.A.
Rivoli, Italy
paolo.ferrero@augeos.it

Andrea Violato
Augeos S.p.A.
Rivoli, Italy
andrea.violato@augeos.it

***Abstract*—This paper describes a practical application of risk assessment in a project involving governance and compliance of Artificial Intelligence and Internet-of-Things solutions in healthcare. The proposed methodology consists of five steps applied to the high performance computing platform used for managing Internet of Medical Things technologies. We describe the architecture of the tool as well as assets, dimensions, and levels of investigation. The main points of interest are discussed. The use case demonstrates the effectiveness of an Information Technology risk assessment process in healthcare organization management.**

***Index Terms*—Enterprise Risk Management, Governance Risk and Compliance, Telehealth, Hospital at Home Service**

I. Introduction

In an increasingly data-driven world, it is essential to support an organization through modern, secure and reliable technologies. Business process management (BPM) [1] focuses on business process lifecycle daily procedures, which are also relevant in Risk Management (RM) [2], [3]. In particular, Enterprise Risk Management focused on risks that face organizations with the aim to improve corporate governance and RM [4], [5], whereas Risk Assessment (RA) allows for the identification of potential risks to a project [6]. In this context, an assessment allows for a risk-informed decision making [7]. Nowadays, the regulatory dimension has become increasingly important and IT tools can help organizations to meet the new standards [8].

The integrated concept of Governance, Risk and Compliance (GRC) successfully enables an organization to manage the three aspects of GRC acronym together [9]. This concept has recently found increasing interest among researchers and practitioners in several areas [10], from finance [11] to industry [12]. Some results have also been explored in healthcare, where there is an urgent need for procedures to contrast data loss, to pursue security, and compliance to norms [13]. These procedures are increasingly complex. For instance, the origin of data breaches can be either directly or indirectly the result of employee carelessness or failure to comply with existing information security regulations and policies [14], as well as due to external attacks.

This paper presents an Information Technology Risk Assessment (ITRA) use case in a telehealth project on hospital-at-home services. In view of the most recent regulations on the protection of privacy, personal data (GDPR) and data breach risks, the proposed methodology allows to perform an IT risk analysis to assess and monitor the components potentially subject to risks. In particular, this work discusses an IT solution to support physicians and patients by bringing together Internet of Medical Things (IoMT) technologies, artificial intelligence (AI) and process management on a high-performance computing research platform (HPC4AI.) Full risk governance requires clarity of purpose, cross-functionality, precision. The GRC platform implemented the ITRA along with ICT staff who helped identify the risks associated with the platform.

In the following of the paper we first introduce the background with related work and the case study (Section II). Then we describe the GRC framework in Section III and the ITRA in Section IV. Section V provides technical insights about the integration of the tool in the RM process. Finally, some discussion on the technological and methodological challenges arisen so far are detailed in Section VI, while Section VII concludes the paper.

II. Background

A. Related work

Existing RA methodologies depend on contexts, the type of organizations, as well as the primary objective (e.g., damage on critical assets versus threat viability) [15]. These approaches can be defined by governments, standards bodies, as well as guidelines or best practices, like e.g. NIST SP800-30 or ISO/IEC 27001. In an organization, regular RA will enable the continuous improvement to advance enterprise-wide risk management [16].

Cyber-physical systems, Artificial Intelligence (AI) and Internet-of-Things (IoT) frameworks are particularly challenging for RM [17], [18]. According to [19], the main issues include:

(i) The periodic nature of assessments [20], requiring consideration of the dynamics of devices currently in use and those that might become connected.

(ii) Because technological changes are sudden and unpredictable, IT professionals can alarmingly identify many more potential risks when many will never materialize.

(iii) Understanding the overall system is not only in the communication protocols and standards, but also in the inner workings of the actors themselves.

(iv) Some assets can become a platform for attack, as they can be attacked and used as distributed cyber-weapons.

These challenges need new approaches to assess risk and build system trust [21]. GRC systems are increasingly used as an integrated and holistic approach [10] to enterprise-wide governance, risk, and compliance [22]. In healthcare, the adoption of IoMT [23] has emphasized the security and privacy [24] of GRC health systems [25], the hospital management perspective [26], as well as healthcare risk communication [27].

B. The use case

Telehealth project. This work is based on a three-year telemedicine project (CANP) involving an IoMT device system for home hospitalization[1]. The technological solutions are based on an HPC platform to facilitate data collection, processing, and return. The particularly challenging nature of CANP was the implementation of a complex technological apparatus resulting from the proactive collaboration of several organizations [28], [29]. In fact, the partners involved were 15 small and medium ICT enterprises, 2 large enterprises, 2 universities (University and Politecnico of Torino), a private research center, and 4 hospitals. The main hospital involved in the project is the City of Health and Science of Turin, one of the most populated cities in Northern Italy. In particular, the Home Hospitalization Service has been in operation for over 30 years, proving its value for a variety of acute and chronic illnesses [30].

Devices and applications of IoMT. The set of ICT solutions involved in the project includes: i. A clinical platform to manage clinical trials information (e.g., data from questionnaires, user input, clinical external platforms.) ii) A solution for enabling remote control of patients, caregivers or staff to perform health care procedures, examination and adherence to therapy. iii) A telemedicine & IoT Platform to collect personal health information and daily activities with the support of integrated environmental sensors, wireless medical devices, secure audio/video connections. iv) A mobile application and web platform for monitoring drugs interactions. v) An application to perform language rehabilitation exercises. vi) A conversational agent for training on some therapeutic practices. vii) An augmented reality mobile application to accompany the caregiver in the use and maintenance of complex medical devices. viii) A wearable device (aesthetically a wristwatch) and a base station acting as home gateway.

HPC4AI. The technological infrastructure HPC4AI [31] is a cloud system for hosting the above mentioned IoT solutions, as well as to collect and facilitate data analysis of telemedicine activities [32].

III. Governance, risk, and compliance solution

A. General framework

Effective RM must balance the needs of both security and reliability required by the nature of the project and completeness and conformity necessary for an effective RM activity. After an initial analysis of the data processing methods within the project perimeter, the focus shifted to an assessment of the technological system and the tools for controlling and combating risks. The initial definition of the analysis perimeter includes the identification of the main IT risk components. In particular, the following entities have been investigated: i) IT assets, meaning all technological applications, databases, IT procedures inherent to the project. ii) Scenarios, threats and vulnerabilities, i.e. the modalities through which it is possible to proceed with circumstantial analysis on the occurrence of risk hypotheses. iii) Controls and countermeasures, i.e. the mitigation and/or contrast activities implemented in order to limit, contrast or remedy the occurrence of risk hypothesis.

B. GRC architecture

The multi-tier architecture infrastructure allows the deployment of the application, as described in Figure 1. The GRC platform includes several modular technological solutions, highly flexible, that can host - even simultaneously - different configurations for the management of operational risk, compliance, governance. Being a common platform for several solutions allows GRC to manage in a homogeneous and centralized way all the cross functional aspects, necessary to the different configurations in place. The configurations can ensure information consistency and functional integrity. More specifically, GRC offers homogeneous and transversal functionalities regarding:

- The profiling and management of the organizational structure.
- The ability to configure synchronization/alignment procedures from third-party sources.
- Management of taxonomies, questionnaires and workflows.
- Management of roles and permissions.

C. GRC implementation

The GRC architecture represents the logical subdivision of the application components. The main implemented software components that constitute the whole application are:

- The data repository is managed on a SQL Server database.
- The ASP.NET Framework application encapsulates:

[1] The CANP project has been funded by a POR FESR UE initiative, see http://casanelparco-project.it/ (accessed 12 Oct 2021.)

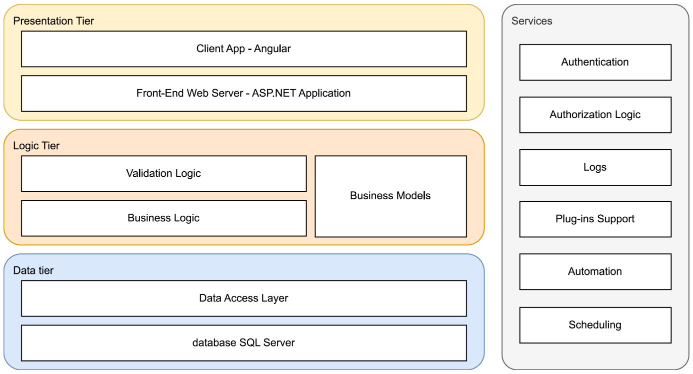


Fig. 1. Logical tiers of GRC architecture

- The entire business logic layer
- The data access layer
- The server-side web API used by the clients
- The static contents that constitute the client application

Finally, the client is available through a web application based on the Angular framework.

D. Modules

The system modules used and adapted in the project are:

- *Risk Shelter*. A platform for the management of operational risks, containing a description of the activities that are 'risky' and potentially generate loss events.
- *ITRM*. This module stores information about company assets, threats and related controls, as well as detailed information and the results of RA.
- *Normageos*. A module for the management of non-compliance risks and in particular for the management of the record of processing and normative issue, like e.g. GDPR.
- Transversal modules for the management of the system's basic master data (users, roles, permissions, organizational units, companies, taxonomies).

In particular, the data stored on the GRC platform concerns user data (e.g., first name, last name, email address), as well as the organizational structure.

IV. Risk assessment

RA is the process of analysing potential threats and vulnerabilities to the IT systems to establish what losses might expect to incur if certain events happen. The objective is to help you achieve optimal security at a reasonable cost.

The ITRA was conducted by applying the methodology here presented together with the above mentioned GRC. The definition and application of a stable methodology is fundamental, in any business project, to support the governance phase. This allows the execution of an Analysis Governance Process, to which all activities and resources must refer in order to set and control the performance in accordance with the project objectives. The methodology adopts a flexible and modular methodological approach that can be summarized in the following operational phases, as in Figure 2.

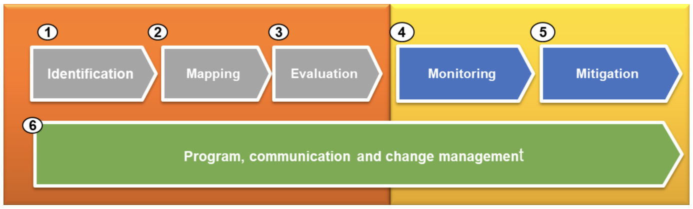


Fig. 2. The phases of the methodological approach

Identification. Identifies all relevant objects that are involved in the IT risk analysis consistent with the objectives stated in the project setup, e.g. People, roles, and organizational units. This phase includes the analysis of: i) IT incidents, complaints, loss accounting events, anomaly reports. ii) IT assets (software procedures, services, databases, infrastructure and tools with their quality objectives.) iii) The categories of risk, threats and vulnerabilities, impact, IT risk factors. iv) Regulatory compliance, internal and external regulations, policies.

Mapping. It concerns the structured allocation of asset risks in business processes, making explicit where they may occur, allowing the creation of a map of the relationships between the objects foreseen in the risk model. This is realized in the identification of relations to two or more dimensions. Examples of two-dimensional relationships are asset-threat or threat-control relationships. Relations with more than one dimension are those, also derived, such as asset-threats-controls.

Evaluation. Evaluates the Risks with ex-ante methodologies (Self RA) and/or ex-post (statistical analysis of events that have occurred.) This operational phase involves the actors who have responsibilities in RM for assigning the impact, probability and adequacy values of the controls necessary to define the risk levels (gross and residual.)

Monitoring. Configures the monitoring system and the methods for measuring the risks identified in the previous phase also with the use of Key Risk Indicators dashboards. Risk monitoring is an activity whose benefit is in its continuous application because it allows to identify punctually, perhaps early, the elements (assets, threats, controls) that determine a level of risk that exceeds certain tolerance thresholds.

Mitigation. Implement mitigation actions that operate on the conditions that determine the critical events to reduce the probability of occurrence and cancel the effects, operating intervention plans and verifying their execution over time.

Program, communication and change management. Transversal phase whose purpose is to transfer, at all levels, in a correct and effective way, the information derived from RA and that allow the right people to make decisions in a correct and informed way.

V. Integrating the tool in Risk Management Process

RA is considered the first activity of a RM process. Best Practice about treating RM refers to the *Deming PDCA cycle* [33]. RA is primarily related to the Plan phase and can be involved in the Check and Act phases. GRC helps the approach of RA as part of PDCA Plan phase, because the methodology is implemented as *reusable set of objects*, inside a RA Session. These objects represents all the elements the Risk Manager has to evaluate in a RA:

- Assets: these objects are the value item that are to be included in the RA, as they can be potentially involved in accidents or damage events. They represent the perimeter of the RA. Any of these object can be assigned to a separated Organizational Unit, represented by a group of users associated within a RA session. These improves Segregation of Duty requisite and can assign the evaluation work to the suitable Asset Manager.
- Threats: they represent the cause of damages that can occur to assets.
- Scenarios: they represents set of impacts/damages that can occur when a threat is applied to an Asset. Scenarios are essential to estimate the real impact on the evaluated perimeter. In an ITRA, typical scenarios are related to data status (Confidentiality, Integrity, Availability)
- Controls: these objects are the countermeasures that can be implemented to mitigate or cancel the probability that a threat can cause a significant damage to an asset.
- Measure Scales: these are the evaluation terms of measure about Probability and Impact that a Threat can occur on an Asset, causing a impact on a Scenario. The scales are defined as qualitative enumerating sets and also numeric values can be assigned to the items.

All these objects are treated as separated item *catalogs*, permanently stored in GRC. Their scope is global to a GRC instance, so that these catalogs can be used to start any RA Session.

Moreover, the RA Sessions are permanently stored with their status about completeness of all the methodology steps. The Risk Manager can jump between states at any time and there is a validation check between any state, that reports any anomaly about inconsistency in evaluation, cross relations and so on. As a RA session is completed, a new RA session can be derived from the completed one. This is very useful in a PDCA Risk Management process in the Check and Act Phase: the second RA can be compared directly with the one completed in the Plan Phase and the results between the supposed mitigation strategy and the implemented one are immediately visible. This way, the Act Phase of correcting the strategy can be implemented easily.

VI. Discussion

The practical application presented in the paper includes several points of interest. We mention here some considerations about some ITRA features pros and cons, the *auditability*, as well as the repercussions on the privacy issue in healthcare.

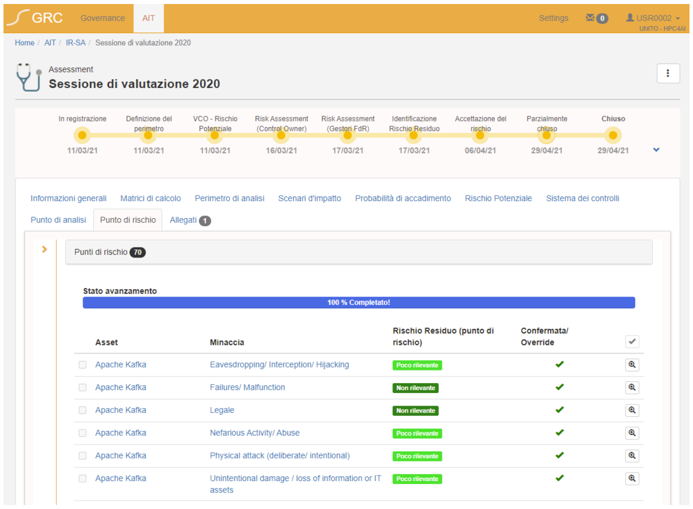
Advantages and disadvantages. The qualitative/quantitative procedure adopted makes it possible to introduce an Assessment that precisely determines the system of controls applied (*asset catalog*) in order to carry out a Control Assessment, to indicate the probability of occurrence of the threats, and finally apply a system of controls. Compared to standards and best practices, this model sees a refined controls level analysis, based on two main drivers: i) the existence of effectiveness (i.e., the capacity of the countermeasures, either contrast or mitigation, in daily life to exert its effects), and ii) regularity (i.e., after having ascertained that it exists and is effective, it is measured how effectively this countermeasure is regular, in accordance with authority, national norms and standards.) One very useful feature is the ability to assign parts of the RA pipeline to *groups* and *roles* entities. This allows users to proceed more directly, without having to contact the people who are doing the work independently. Another advantage is the possibility to reuse parts of the process through the “templating” functionality of the RA. This avoids having to rely solely on external documents, and trying to reconstruct the history of part of the evaluation by rereading the documentation (this procedure can leave significant errors in the reconstruction.) Finally, the experience demonstrates the usefulness of such an ITRA tool for thinning out the threats. In fact, users with little RA experience may initially indicate too many threats and overestimate the risk. This would need more rounds of accommodation and reduction in numerosity, wasting time. Some suggestions for improvement relate to adopting a scale that can be applied to cascading controls, as well as to enhance the graphics section, perhaps with heat-maps in the dashboard.

Audit-proof system. A relevant aspect of the current approach is that allows the board and the lenders (for project audits) to access a report on the product that was created as a summary for having a big picture easy to consult. Every object inside an ITRA session can have a document file attached, so that every point of attention in the assessment can be motivated. Unlike typical methods using raw representation in tables and spreadsheets, this assessment becomes auditable/accountable. In fact, ITRA helps in case of audits or inspections by internal or external supervisory bodies to reconstruct and justify the choices made through specific logs and records of changes of any significant element of the analysis. An opportune representation of the results improves the understanding, like in the example provided in Figure 3.

ITRA in itinere. Instead of doing a proof-of-concept through prototypes, in this project the ITRA was done *in itinere*. The output of the CANP project is a set of technologies working for clinicians on HPC4AI, the container platform of the technology stack. The proposed ITRA demonstrated that already the prototyping phase is consistent with the standards (e.g., with GDPR, system of controls, cyber security.) The assessment as early as conceptualization certifies that the product of the project is already consistent with real world standards.

Privacy issues in healthcare. A relevant point of attention is the issue of privacy, which is becoming increasingly relevant in healthcare. The ITRA system allows to keep under control the privacy threats as the legislation after GDPR has become very strict. The tool allows managers not to miss some controls and also helps streamline the methodology.

Project management. In a project with multiple partners, the



	Asset	Minaccia	Rischio Residuo (punto di rischio)	Confermata/ Override	✓
□	Apache Kafka	Eavesdropping/ Interception/ Hijacking	Poco rilevante	✓	🔍
□	Apache Kafka	Failures/ Malfunction	Non rilevante	✓	🔍
□	Apache Kafka	Legale	Non rilevante	✓	🔍
□	Apache Kafka	Nefarious Activity/ Abuse	Poco rilevante	✓	🔍
□	Apache Kafka	Physical attack (deliberate/ intentional)	Poco rilevante	✓	🔍
□	Apache Kafka	Unintentional damage / loss of information or IT assets	Poco rilevante	✓	🔍

Fig. 3. The final map of risk points as intersections between impact probability and applied controls (text in Italian)

GRC facilitates coordination and collaboration, being a multi-partner and multi-role tool. The above mentioned experience makes it possible to assess the effectiveness of increasing integration of an IT risk management process even within research projects, for which regulations are less restrictive and binding.

VII. Conclusions and Future Works

This paper described a methodology for ITRA applied in an AI and IoT healthcare project, demonstrating the usefulness of such a tool instead of traditional spreadsheet-based AR. The use case demonstrates how introduce RM topics to technical staff of an ICT organization. The next step is to apply a maturity model, which was not applied here because this was the first attempt at ITRA for the organization's staff involved in the project. In fact, the staff (process owners) are technical figures who were not familiar with these concepts and tools. The model applied here has allowed the introduction of a "company culture" capacity to address the issue of *risks*, which through the proposed tool have approached the RM and will therefore be able to carry out the maturity model.

Another future work is to improve the current tool with the inclusion of controls within processes, from a BPM perspective, in order to have an RA that can be updated automatically. Finally, it would be helpful to have pre-mapping between controls, countermeasures, and risks already available (e.g., on ISO 27001 categories). This can help to automatically load risks and threat categories if the user has no previous experience.

Acknowledgement

This research has been partially carried out within the "Circular Health for Industry" project funded by "Compagnia di San Paolo" under the call "IA, uomo e società" and the project "CANP - CAsa Nel Parco" of Regione Piemonte funded by POR FESR PIEMONTE 2014-2020.

References

[1] M. Dumas, M. La Rosa, J. Mendling, and H. Reijers, *Fundamentals of Business Process Management*, 2nd ed. Springer, 2018, vol. 1.

[2] M. Zur Muehlen and D. T.-Y. Ho, "Risk management in the bpm lifecycle," in *International Conference on Business Process Management*. Springer, 2005, pp. 454–466.

[3] E. Sulis, I. A. Amantea, and G. Fornero, "Risk-aware business process modeling: A comparison of discrete event and agent-based approaches," in *Winter Simulation Conference, National Harbor, MD, USA, December 8-11, 2019*. IEEE, 2019, pp. 3152–3159.

[4] D. L. Olson and D. D. Wu, *Enterprise risk management*. World Scientific Publishing Company, 2015, vol. 3.

[5] I. Coso, "Enterprise risk management-integrated framework," *Committee of Sponsoring Organizations of the Treadway Commission*, vol. 2, 2004.

[6] E. Zio, "The future of risk assessment," *Reliability Engineering & System Safety*, vol. 177, pp. 176–190, 2018.

[7] T. Aven and E. Zio, *Knowledge in risk assessment and management*. John Wiley & Sons, 2018.

[8] R. Conforti, G. Fortino, M. L. Rosa, and A. H. M. ter Hofstede, "History-aware, real-time risk detection in business processes," in *On the Move to Meaningful Internet Systems: OTM 2011 - Confederated International Conferences: CoopIS, DOA-SVI, and ODBASE 2011, Hersonissos, Crete, Greece, October 17-21, 2011, Proceedings, Part I*, ser. Lecture Notes in Computer Science, R. Meersman, T. S. Dillon, P. Herrero, A. Kumar, M. Reichert, L. Qing, B. C. Ooi, E. Damiani, D. C. Schmidt, J. White, M. Hauswirth, P. Hitzler, and M. K. Mohania, Eds., vol. 7044. Springer, 2011, pp. 100–118. [Online]. Available: https://doi.org/10.1007/978-3-642-25109-2_8

[9] A. Papazafeiropoulou and K. Spanaki, "Understanding governance, risk and compliance information systems (grc is): The experts view," *Information Systems Frontiers*, vol. 18, no. 6, pp. 1251–1263, 2016.

[10] N. Racz, J. Panitz, M. Amberg, E. Weippl, and A. Seufert, "Governance, risk & compliance (grc) status quo and software use: Results from a survey among large enterprises," 2010.

[11] M. P. Cangemi, "The controls challenge: automation can cut costs and make processes more consistent," *Bank accounting & finance*, vol. 21, no. 5, pp. 43–46, 2008.

[12] N. Racz, E. Weippl, and R. Bonazzi, "It governance, risk & compliance (grc) status quo and integration: An explorative industry case study," *2011 IEEE World Congress on Services*, pp. 429–436, 2011.

[13] I. A. Amantea, A. Di Leva, and E. Sulis, "A simulation-driven approach in risk-aware business process management: A case study in healthcare." in *SIMULTECH*, 2018, pp. 98–105.

[14] S. R. Kessler, S. Pindek, G. Kleinman, S. Andel, and P. E. Spector, "Information security climate and the assessment of information security risk among healthcare employees," *Health Informatics J.*, vol. 26, no. 1, 2020. [Online]. Available: https://doi.org/10.1177/1460458219832048

[15] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (isra)," *Computers & security*, vol. 57, pp. 14–30, 2016.

[16] N. Azizi and K. Hashim, "Enterprise level it risks: An assessment framework and tool," in *2010 3rd International Conference on Computer Science and Information Technology*, vol. 3. IEEE, 2010, pp. 333–336.

[17] P. Radanliev, D. C. De Roure, R. Nicolescu, M. Huth, R. M. Montalvo, S. Cannady, and P. Burnap, "Future developments in cyber risk assessment for the internet of things," *Computers in Industry*, vol. 102, pp. 14–22, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0166361518301817

[18] J. Nurse, P. Radanliev, S. Creese, and D. D. Roure, "If you can't understand it, you can't properly assess it! the reality of assessing security risks in internet of things systems," *IET Conference Proceedings*, pp. 1 (9 pp.)–1 (9 pp.)(1), 1 2018. [Online]. Available: https://digital-library.theiet.org/content/conferences/10.1049/cp.2018.0001

[19] J. R. Nurse, S. Creese, and D. De Roure, "Security risk assessment in internet of things systems," *IT Professional*, vol. 19, no. 5, pp. 20–26, 2017.

[20] S. Taubenberger, J. Jürjens, Y. Yu, and B. Nuseibeh, "Problem analysis of traditional it-security risk assessment methods–an experience report from the insurance and auditing domain," in *IFIP International Information Security Conference*. Springer, 2011, pp. 259–270.

[21] H. Abie and I. Balasingham, “Risk-based adaptive security for smart iot in ehealth,” in *Proceedings of the 7th International Conference on Body Area Networks*, 2012, pp. 269–275.

[22] M. Nicho, S. Khan, and M. Rahman, “Managing information security risk using integrated governance risk and compliance,” in *2017 International Conference on Computer and Applications (ICCA)*. IEEE, 2017, pp. 56–66.

[23] Y. YIN, Y. Zeng, X. Chen, and Y. Fan, “The internet of things in healthcare: An overview,” *J. Ind. Inf. Integr.*, vol. 1, pp. 3–13, 2016.

[24] J. L. Fernández-Alemán, I. C. Señor, P. Ángel Oliver Lozoya, and A. Toval, “Security and privacy in electronic health records: A systematic literature review,” *Journal of Biomedical Informatics*, vol. 46, no. 3, pp. 541–562, 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1532046412001864

[25] R. Wilton, “Trust and ethical data handling in the healthcare context,” *Health and Technology*, vol. 7, no. 4, pp. 569–578, 2017.

[26] R. Batenburg, M. Neppelenbroek, and A. Shahim, “A maturity model for governance, risk management and compliance in hospitals,” *Journal of Hospital Administration*, vol. 3, no. 4, pp. 43–52, 2014.

[27] R. E. Lundgren and A. H. McMakin, *Risk communication: A handbook for communicating environmental, safety, and health risks*. John Wiley & Sons, 2018.

[28] I. A. Amantea, M. Arnone, A. Di Leva, E. Sulis, D. Bianca, E. Brunetti, and R. Marinello, “Modeling and simulation of the hospital-at-home service admission process,” in *SIMULTECH*, 2019, pp. 293–300.

[29] E. Sulis, I. A. Amantea, G. Boella, R. Marinello, D. Bianca, E. Brunetti, M. Bo, A. Bianco, F. Cattel, C. Cena *et al.*, “Monitoring patients with fragilities in the context of de-hospitalization services: An ambient assisted living healthcare framework for e-health applications,” in *23rd ISCT*. IEEE, 2019, pp. 216–219.

[30] G. Isaia, V. Tibaldi, M. Astengo, M. Ladetto, R. Marinello, M. Bo, G. Michelis, F. Ruatta, and N. A. Ricauda, “Home management of hematological patients requiring hospital admission,” *Arch. Gerontol. Geriatr.*, vol. 51, no. 3, pp. 309–311, 2010.

[31] M. Aldinucci, S. Rabellino, M. Pironti, F. Spiga, P. Viviani, M. Drocco, M. Guerzoni, G. Boella, M. Mellia, P. Margara, I. Drago, R. Marturano, G. Marchetto, E. Piccolo, S. Bagnasco, S. Lusso, S. Vallero, G. Attardi, A. Barchiesi, A. Colla, and F. Galeazzi, “HPC4AI: an ai-on-demand federated platform endeavour,” in *Proceedings of the 15th ICCF, Ischia, Italy, May 08-10, 2018*, D. R. Kaeli and M. Pericàs, Eds. ACM, 2018, pp. 279–286.

[32] I. A. Amantea, E. Sulis, G. Boella, R. Marinello, D. Bianca, E. Brunetti, M. Bo, and C. Fernandez-Llatas, “A process mining application for the analysis of hospital-at-home admissions,” *Studies in health technology and informatics*, vol. 270, p. 522—526, Jufne 2020.

[33] P. M. Swamidass, Ed., *PDCA (Plan, Do, Check, Act)PLAN-DO-CHECK ACT (PDCA)*. Boston, MA: Springer US, 2000, pp. 523–523. [Online]. Available: https://doi.org/10.1007/1-4020-0612-8_689