L-SQUARE: Preliminary Extension of the SQUARE Method to Address Legal Compliance

Nancy Mead
Aaron Alva
Lisa Young

Notices

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0001561

Topics

About CERT/SEI/CMU

Author bios

Speaker bio

SQUARE overview & SQUARE steps

Extending SQUARE for legal compliance

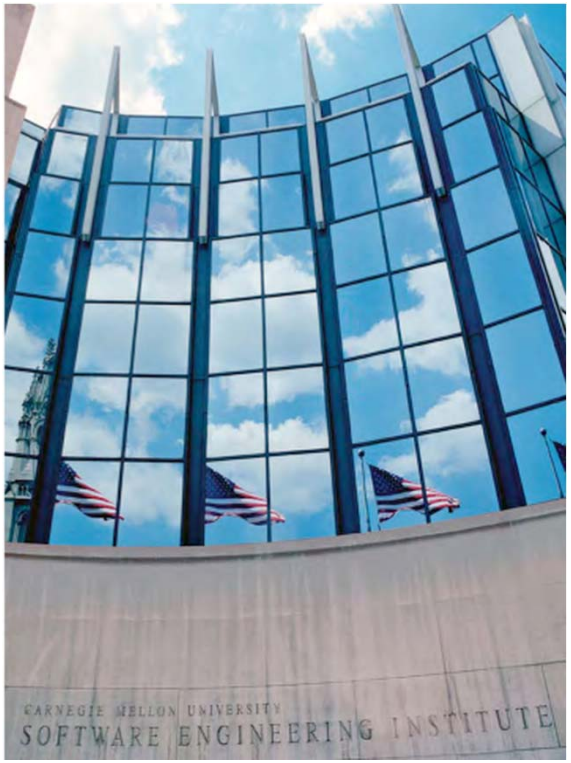
The need for legal compliance

Example legal requirements

L-SQUARE steps & considerations

Questions

CERT | Software Engineering Institute | Carnegie Mellon



Carnegie Mellon University

Software Engineering Institute (SEI)

- Federally funded research and development center based at Carnegie Mellon University
- Basic and applied research in partnership with government and private organizations
- Helps organizations improve development, operation, and management of software-intensive and networked systems

CERT – *Anticipating and solving our nation's cybersecurity challenges*

- Largest technical program at SEI
- Focused on information security, digital investigation and forensics, building secure systems and software, insider threat, operational risk, vulnerability analysis, network situational awareness, metrics, and governance

SEI CERT Cyber Risk Management Team

Operational Risk Management

Ensuring Operational Mission Success

Resilience Management Frameworks

To define, validate, and evolve frameworks that enable stakeholders to make data driven decisions for measuring, communicating, strengthening, and maintaining their cybersecurity and risk management posture

Measurement & Data Analytics

To research, design, and develop measurement and analysis methods to enable data-driven operational risk management decisions

Policy & Governance

To define the programmatic governance to support operational risk management programs and enable stakeholders to make data driven decisions about cybersecurity and operational risk management policy

Supply Chain Risk Management

To develop and put into practice methods for organizations to improve their supply chain risk management capabilities

Critical Infrastructure Protection

To develop scientifically rigorous methods and evaluation techniques to allow decision makers within critical infrastructures to manage operational risk

Recognized Thought Leaders & Trusted Agents

Author bios

Aaron Alva – is a cybersecurity researcher at the University of Washington, and is affiliated with CERT at Carnegie Mellon University. Aaron is pursuing a Juris Doctor (law) and Masters of Science in Information Management at the UW. His work focuses on legal requirements engineering, digital evidence admissibility, and cloud forensics. Aaron is a contributor to the American Bar Association's Information Security Committee, and is a US National Science Foundation CyberCorps scholarship recipient.

Lisa Young - is a senior engineer at CERT in the Software Engineering Institute at Carnegie Mellon University where she serves as a contributing developer of the Resilience Management Model (RMM). She holds the designation of Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP) and is experienced in IT governance, audit, security and risk management. Lisa teaches the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE®) assessment methodology at the Software Engineering Institute and also teaches operational risk management at the CIO and CISO Institutes for the Heinz College at Carnegie Mellon University.

Speaker bio

Thank you again Nancy!

Nancy R. Mead is a Fellow and Principal Researcher at the Software Engineering Institute (SEI). Mead is an Adjunct Professor of Software Engineering at Carnegie Mellon University. She is currently involved in the study of security requirements engineering and the development of software assurance curricula.

Summary

We introduce **L-SQUARE**, an extension of the SQUARE methodology that may be useful for highly-regulated organizations to conduct requirements engineering particular to legal compliance.

- This methodology's main purpose is to ensure due diligence that the system or software being developed complies with applicable laws or regulations.

Our paper also provides a non-exhaustive review of existing research efforts in requirements engineering and the law.

- These research efforts are discussed for each step in the L-SQUARE methodology.
- L-SQUARE is designed to operate separately from SQUARE, except where explicitly noted.

SQUARE methodology overview

Provides a step-by-step process for "eliciting and prioritizing" security requirements so that such requirements are baked-into software and systems early in the life cycle.

SQUARE has been extended twice already to address acquisition and privacy requirements.

A-SQUARE - Acquisition

P-SQUARE - Privacy

Security **Qua**lity **R**equirements **E**ngineering

SQUARE steps

1. Agree on definitions.
2. Identify assets and security goals.
3. Develop artifacts to support security requirements definition.
4. Assess risks.
5. Select elicitation techniques.
6. Elicit security requirements.
7. Categorize requirements.
8. Prioritize requirements.
9. Inspect requirements.

The need for legal compliance

Organizations in **regulated fields** should address legal compliance when developing software, engineering systems or acquiring software.

The L-SQUARE method is targeted at organizations that are in regulatory-heavy industries that wish to ensure a robust consideration of legal requirements over and above what is required for security or privacy.

- e.g. US finance, healthcare, and energy critical infrastructure sectors

Example legal requirements and penalties

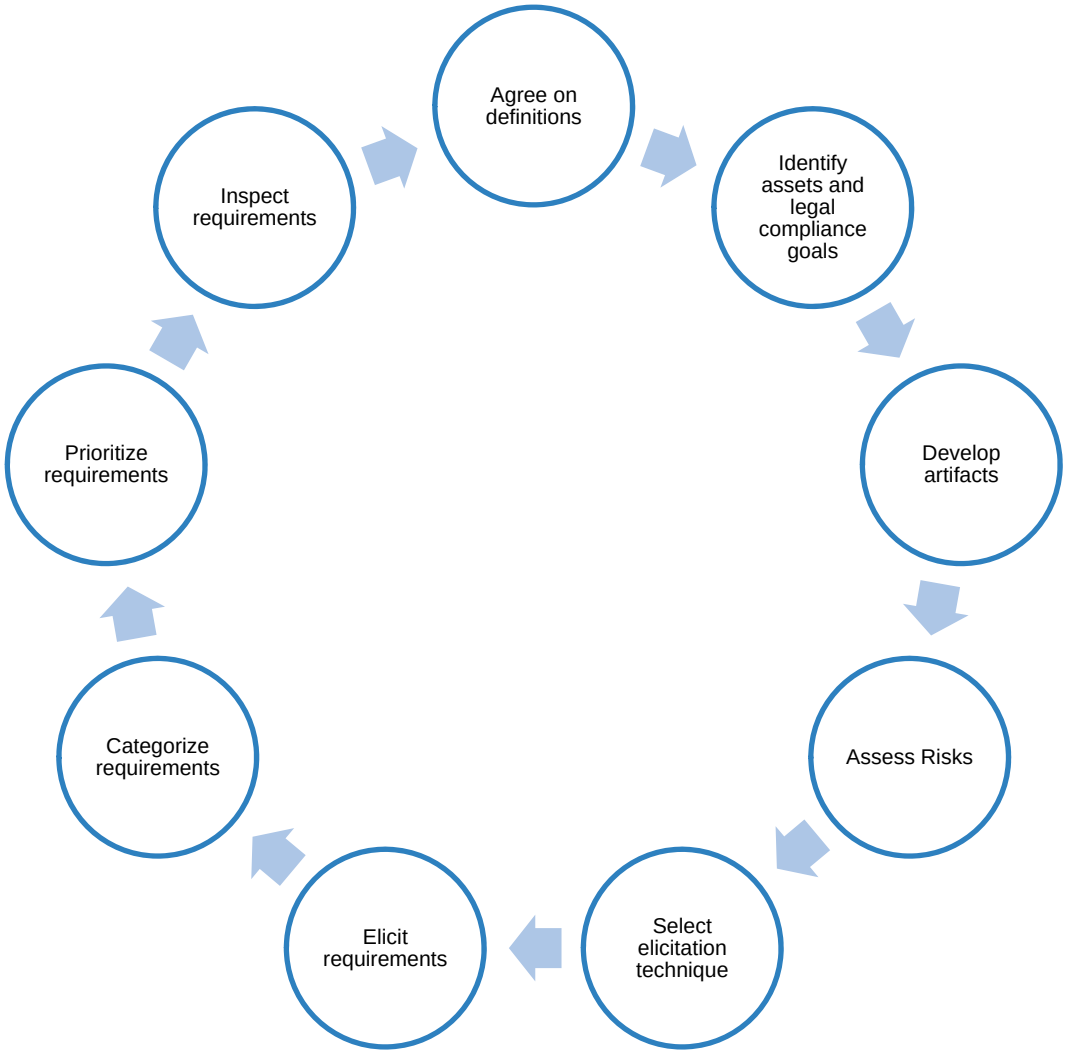
The U.S. healthcare sector must consider the Healthcare Portability and Accountability Act (HIPAA).

The U.S. energy sector must consider a series of regulations, depending on the facet of the business in which they operate.

The financial sector must comply with various financial regulations including the Gramm-Leach-Bliley Act.

- Non-compliance can result in civil or criminal actions against organizational leaders and severe fines ranging from $100K to $250K per occurrence.

L-SQUARE steps



L-SQUARE step 1 considerations

Agree on definitions to reduce ambiguity.

For laws and regulations, defining legal terms in the context of requirements engineering may be difficult. Legal terms may be domain-specific and used differently across multiple laws or regulations.

We recommend delaying this step until you are able to answer the question: *What laws or regulations must the organization comply with?*

L-SQUARE step 2 considerations

Identify legal compliance goals.

Stakeholders should preliminarily identify laws and regulations that are known to apply to the organization.

- This would provide a broad scope by which the requirements engineering process could proceed.

From the initial set of applicable identified laws, the requirements analyses should link the legal goals to security & privacy goals expressed by the organization.

- In doing so, L-SQUARE links to traditional SQUARE as well as P-SQUARE methodologies.
- It serves to align necessary compliance goals with desired organizational goals.

L-SQUARE step 3 considerations

Develop artifacts.

The primary misuse case we selected for the paper is non-compliance.

In the misuse case of non-compliance the organization identifies and documents defensible alternatives to compliance with the actual legal text, such as compensating controls.

- This decision would arise particularly where an organization has competing regulations with which they must comply.

We recommend delaying this step until after Step 8 when the organization should have sufficient information in order to provide traceability to its decisions.

L-SQUARE step 4 considerations

Assess risks.

We recommend this as a first step.

- If the risk of legal non-compliance is low, or the organization can show the security or privacy goals meet legal compliance goals sufficiently, then the remainder of the L-SQUARE process may be unnecessary.

L-SQUARE step 5/6 considerations

Step 5 - Select elicitation technique.

Step 6 - Elicit legal compliance requirements.

Nothing new to add here.

SQUARE does not dictate which elicitation technique should be selected.

- The selection of a particular technique may depend of a number of factors including:
  - the type of legal text (law, regulation, standard, contract, or more);
  - the way the legal text is written (prescriptive, goals-based, standards-based);
  - whether the legal texts are omnibus (such as HIPAA) or are multi-jurisdiction (such as the 47 different state data breach notification laws in the U.S.);
  - and more.

L-SQUARE step 7 considerations - 1

Categorize requirements.

There are minimally five groupings used in SQUARE to categorize requirements: 1) essential; 2) non-essential; 3) software requirements; 4) system requirements; or 5) architectural or infrastructure requirements.

SQUARE is typically for software or system requirements, *not* architectural requirements.

For multi-jurisdiction requirements, this step would also involve the process of joining, disjoining, or providing a minimum requirement that incorporates the multiple laws.

- This could identify high-water mark or low-water mark requirements in preparation for the next step, prioritization.

L-SQUARE step 7 considerations - 2

Categorize requirements – continued.

There are a variety of ways to solve conflicts between legal requirements that, if unresolved, may result in non-compliance. The SQUARE methodology lists a number of requirements solicitation techniques, many of which discuss ways to resolve conflicts.

L-SQUARE step 8 considerations - 1

Prioritize requirements.

The need to be legally compliant should be delineated from the need to have a system properly designed to be secure and privacy-preserving.

We caution that during the prioritization process (step 8) the legal compliance requirements be considered alongside security and privacy requirements by taking into account the identified risks, costs, and benefits.

There is an open research question as to how to prioritize legal compliance requirements compared to security and privacy requirements.

L-SQUARE step 8 considerations - 2

There are at least four possible scenarios for the relationship **between a legal compliance requirement and a security requirement** that require prioritization between legal compliance and the security/privacy requirement:

1. Legal compliance & security requirements *match*
2. Legal compliance requirements *fall below* security requirement.
3. Legal compliance requirements can be *greater than* the identified security requirement.
4. Legal compliance requirements may *not match* security requirements or be necessary for achieving security goal

L-SQUARE step 8 considerations - 3

- Example of legal compliance requirements *not* matching security requirements or goals:

In Washington State, for a processor, business, or vendor to be protected from liability after a breach, they must be certified as PCI (Payment Card Industry) compliant.

So, an organization developing software or systems that involve certain types of payment devices must certify as PCI compliant even though they process no credit card payments.

In this case, PCI certification is the legal compliance requirement, but is unnecessary to meet security goals.

L-SQUARE step 9 considerations

Inspect requirements.

The main goal of this step is to ensure that each requirement elicited from laws or regulations maintains traceability back to the goal of legal compliance. By including this step, L-SQUARE reinforces the need for traceability between legal texts and elicited legal requirements. For traceability to be achieved, ambiguities in legal texts, when translated to legal requirements, should be checked and made explicit when possible.

Questions

Additional resources

Software Security Engineering: A Guide for Project Managers
Addison Wesley. Available from Amazon.

BSI content on requirements engineering:
https://buildsecurityin.us-cert.gov/

SQUARE technical reports:
www.sei.cmu.edu

Contact information

Nancy Mead

SEI Fellow, Principal Researcher

nrm@sei.cmu.edu

Lisa Young

CERT Cyber Risk Management Team

lry@cert.org

Aaron Alva

aalva@uw.edu

SEI Customer Relations

For general inquiries

customer-relations@sei.cmu.edu

412-268-5800

www.cert.org

References

N. Mead, E. Hough, T. Stehney II, "Security Quality Requirements Engineering," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, Technical Report CMU/SEI-2005-TR-009, 2005. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=7657

Jureta, T. Breaux, A. Siena, and D. Gordon, “Toward benchmarks to assess advancement in legal requirements modeling,” *Sixth International Workshop on Requirements Engineering and Law (RELAW),* pp. 25–33, 2013.

D. G. Gordon and T. D. Breaux, “Comparing requirements from multiple jurisdictions,” *Fourth International Workshop on Requirements Engineering and Law (RELAW),* pp. 43–49, 2011

T. D. Breaux and D. G. Gordon, “Preserving traceability and encoding meaning in legal requirements extraction,” *Sixth International Workshop on Requirements Engineering and Law (RELAW),* pp. 57–60, 2013.