Estimating Computer Security Sources of Effort: a Systematic Review

2018 Annual Research Review

Elaine Venson

Advisor: Dr. Barry Boehm

Smiths Medical confirms drug pump vulnerable to cyberhacking

Firm is latest device maker to acknowledges problems; no hacking reports yet received.

By Joe Carlson Star Tribune | SEPTEMBER 18, 2017 — 7:51PM

Cybercrime

Massive ransomware cyber-attack hits nearly 100 countries around the world

ROBOT SECURITY VULNERABILITIES POSE SERIOUS THREAT TO HUMANS

BY ANTHONY CUTHBERTSON ON 3/1/17 AT 9:00 AM

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Equifax breach could be most costly in corporate history

Equifax Inc said it expects costs related to its massive 2017 data breach to surge by $275 million this year, suggesting the incident at the credit reporting bureau could turn out to be the most costly hack in corporate history.

MAR 02 2018

Software Security

- **Definition**: engineering software that continues working under malicious attack [McGraw, 2004]
- Software is a **central and critical aspect** of the computer security problem [McGraw, 2013]
- Many issues faced in computer security today are **rooted in our approach** to developing software and systems [Heitzenrater, 2016]

Software Security vs Application Security

Software Security	Application Security
Proactive Build security in Preventive costs	Reactive Build security around Corrective costs
• Design for security • Testing for security • Software security education	• Network centric approach • Protect software after development • Finding and fixing security issues

What is the most effective way to protect software?

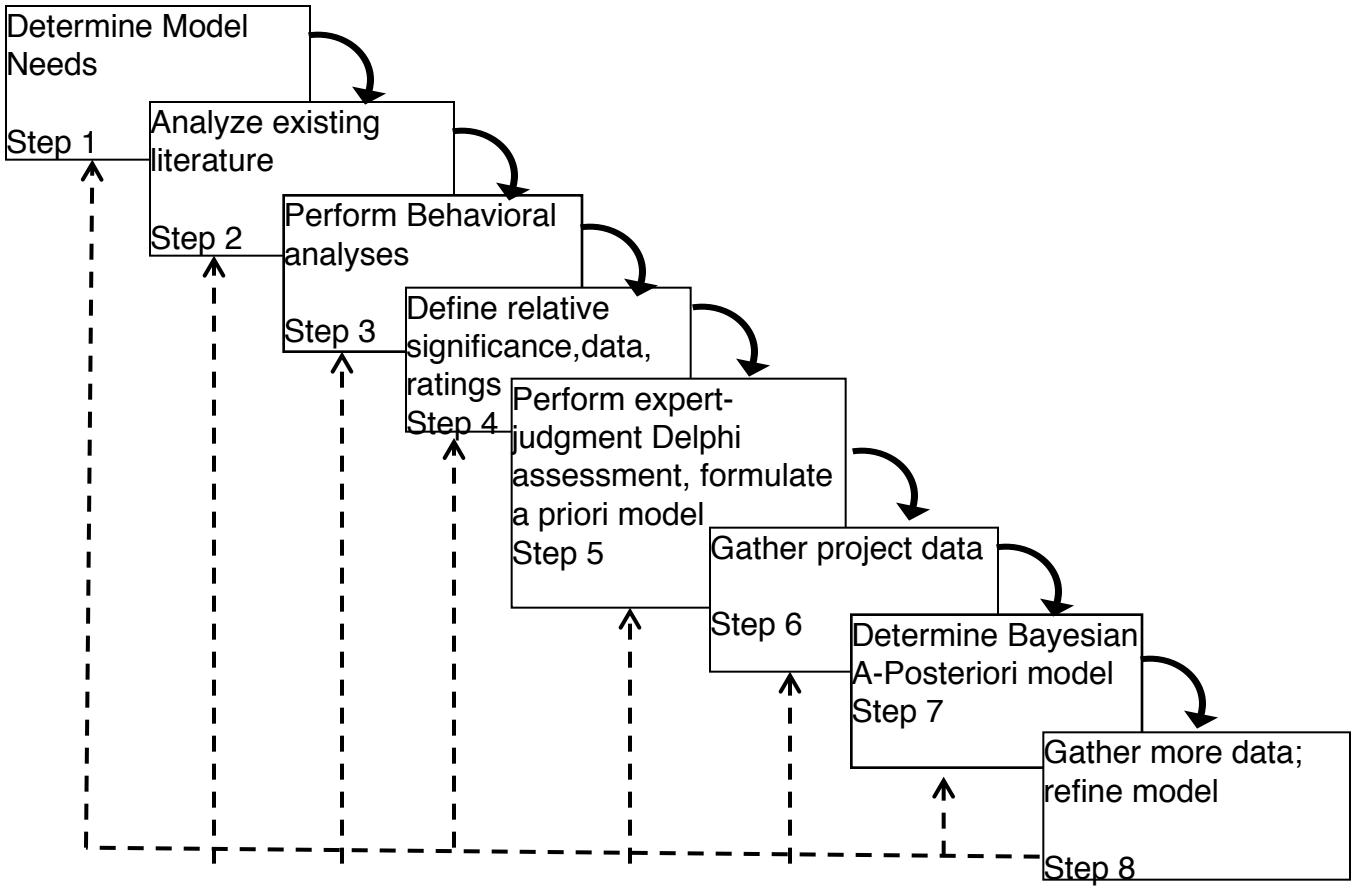
Software Security

- Security remains largely focused on post-development measures late in the SDLC [Heitzenrater, 2016]
- Building secure software is better than protecting bad software
- Cyber war is inevitable, unless we build security in [McGraw, 2013]

Estimating Software Security

- Challenges [Yang, 2015]:
  - Lack of validated methods or models for estimation of secure software systems
  - Large variation in existing security standards
  - Lack of historical data to validate methods
- SW Security solutions face financial and technical barriers, need of thorough approach to planning and execution [Heitzenrater, 2016]
- COCOMO III Security Cost Driver

USC-CSSE Modeling Methodology



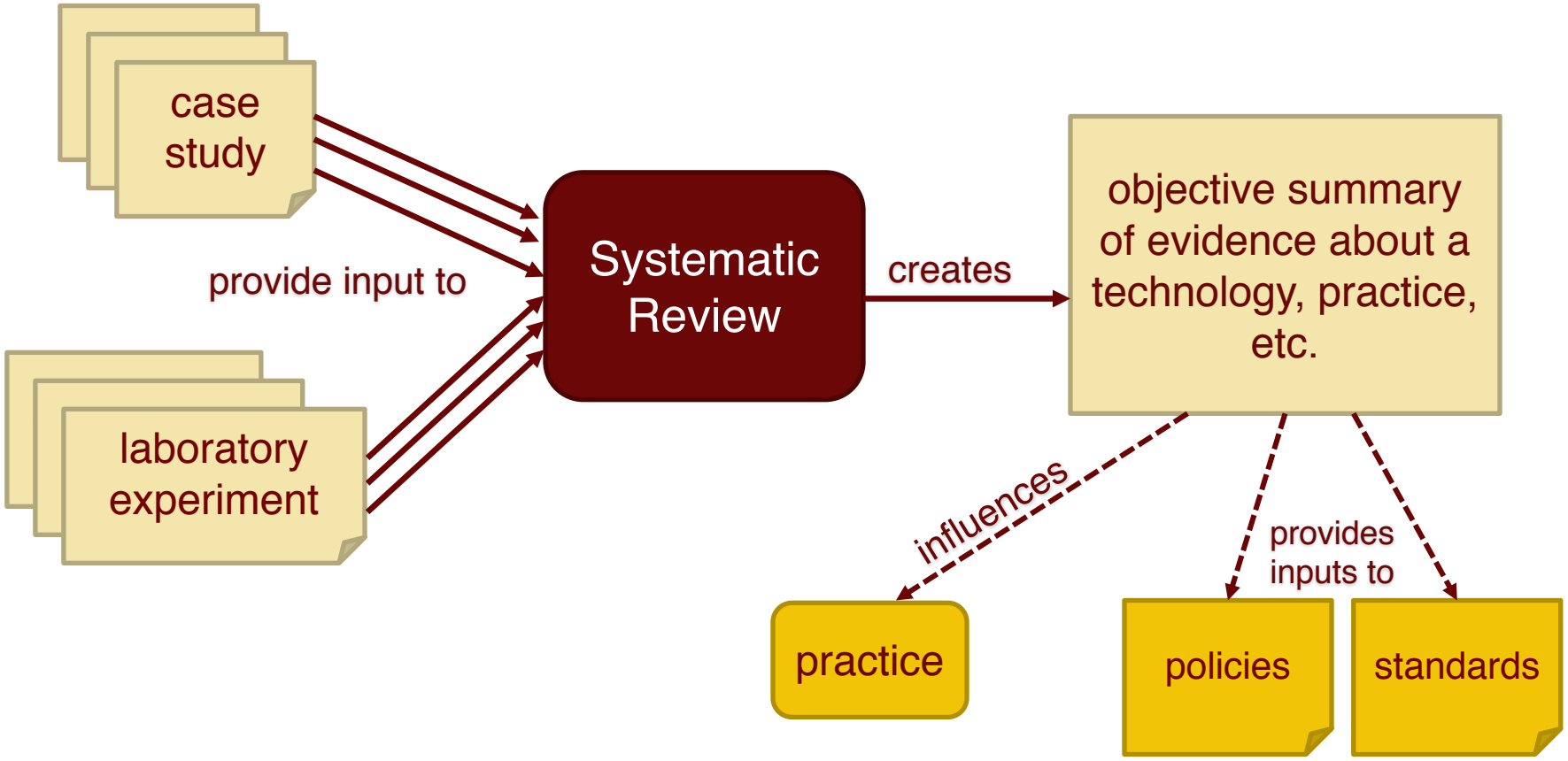
Source: Boehm, B. Software Engineering Economics, Prentice-Hall, Upper Saddle River NJ (1981)

Systematic Review on Security Costs

- Search and identify **all relevant material** related to Software Security Cost Estimation
- Follow objective, analytical and repeatable **procedures**
- A ***secondary study*** -> generate outcomes by aggregating material from ***primary studies***

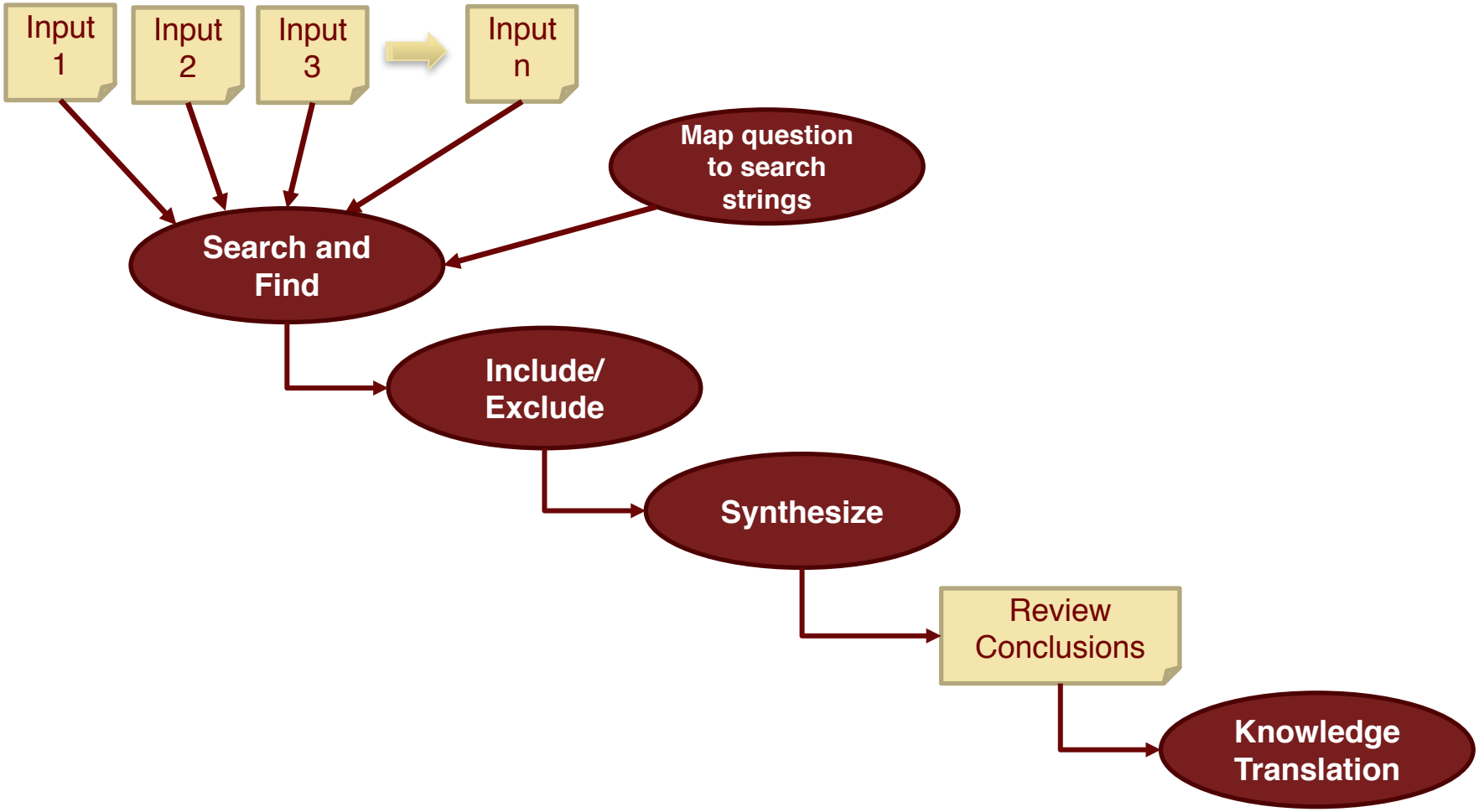
Context of a Systematic Review

Primary Studies



Source: Kitchenham, B.A., Budgen, D., Brereton, P.: Evidence-Based Software Engineering and Systematic Reviews (adapted).

Systematic Review Process



Source: Kitchenham, B.A., Budgen, D., Brereton, P.: Evidence-Based Software Engineering and Systematic Reviews (adapted).

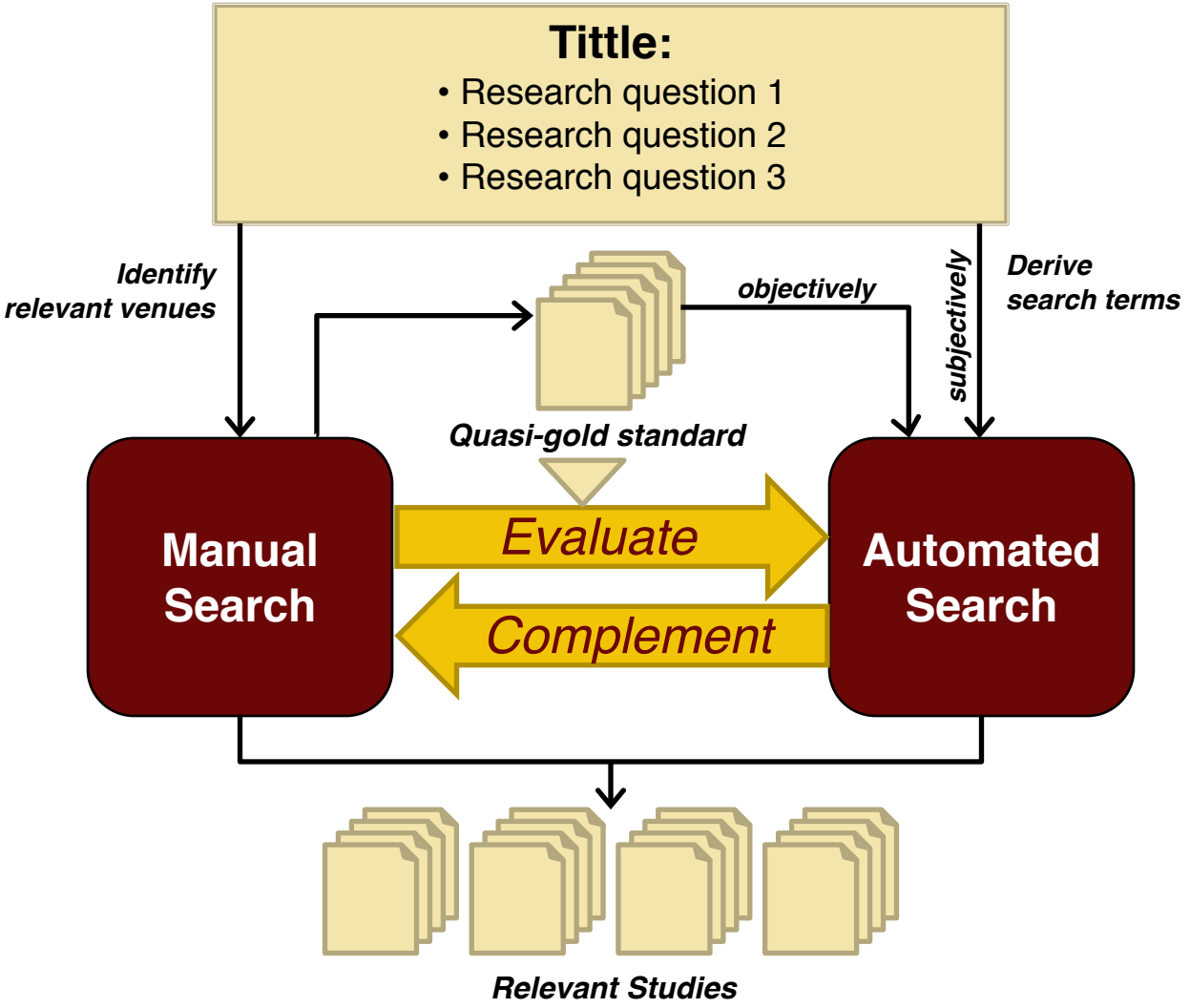
Research Questions

1. Which **papers** report experiences of measuring or estimating the cost of software security requirements in software development projects?
2. What are **the major sources of effort** in developing secure software?
3. What **approaches** have been used to estimate the costs of security in software development projects?
4. Which **data sets** have been used to analyze the cost of secure software?

Research Questions (cont)

5. Which and how **cost drivers** are affected by security requirements?
6. What **issues** have been observed when measuring or estimating costs for secure software development?
7. Which software **security standards** and formal assessments have been used to evaluate costs of secure costs?

Mechanism of the Search



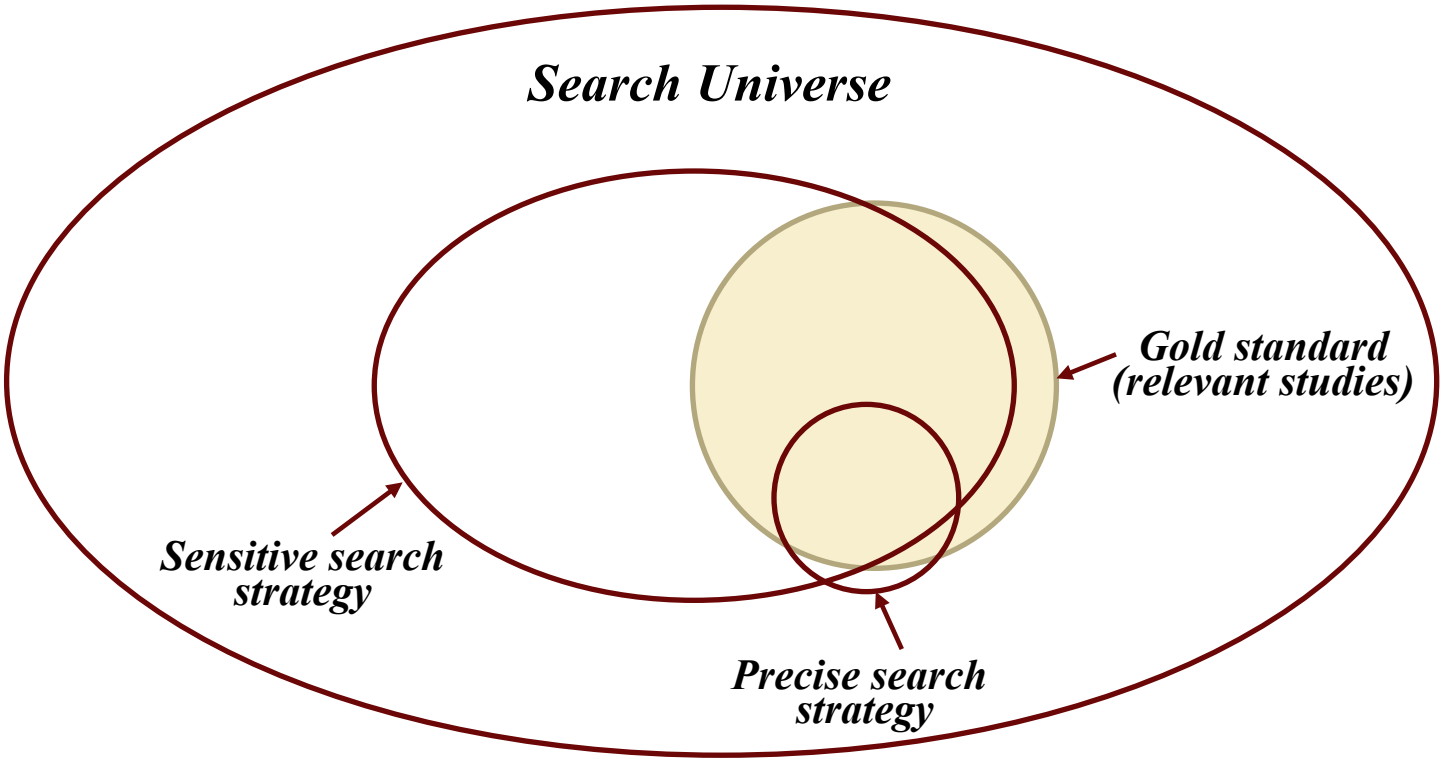
Source: Zhang, H., Babar, M.A., Tell, P.: Identifying relevant studies in software engineering (adapted).

Venues of Search

Manual Search	Automated Search
• IEEE Transactions on Software Engineering (TSE) • ACM Transactions on Software Engineering Methodology (TOSEM) • Empirical Software Engineering Journal • Journal of Systems and Software • Information and Software Technology • Proceedings of the International Conference on Software Engineering (ICSE) • Empirical Software Engineering and Metrics Conference (ESEM) • Workshop on Software Engineering for Secure Systems (SESS) • Software and Systems Modeling • Journal of Cyber Security and Information Systems	• IEEE Digital Library • ACM Digital Library • SpringerLink • Scopus • Web of Science

Completeness: Sensitivity & Precision

Sensitivity	***Precision***
$= \frac{Number\ of\ relevant\ studies\ retrieved}{Total\ number\ of\ relevant\ studies} 100\%$	$= \frac{Number\ of\ relevant\ studies\ retrieved}{Number\ of\ studies\ retrieved} 100\%$

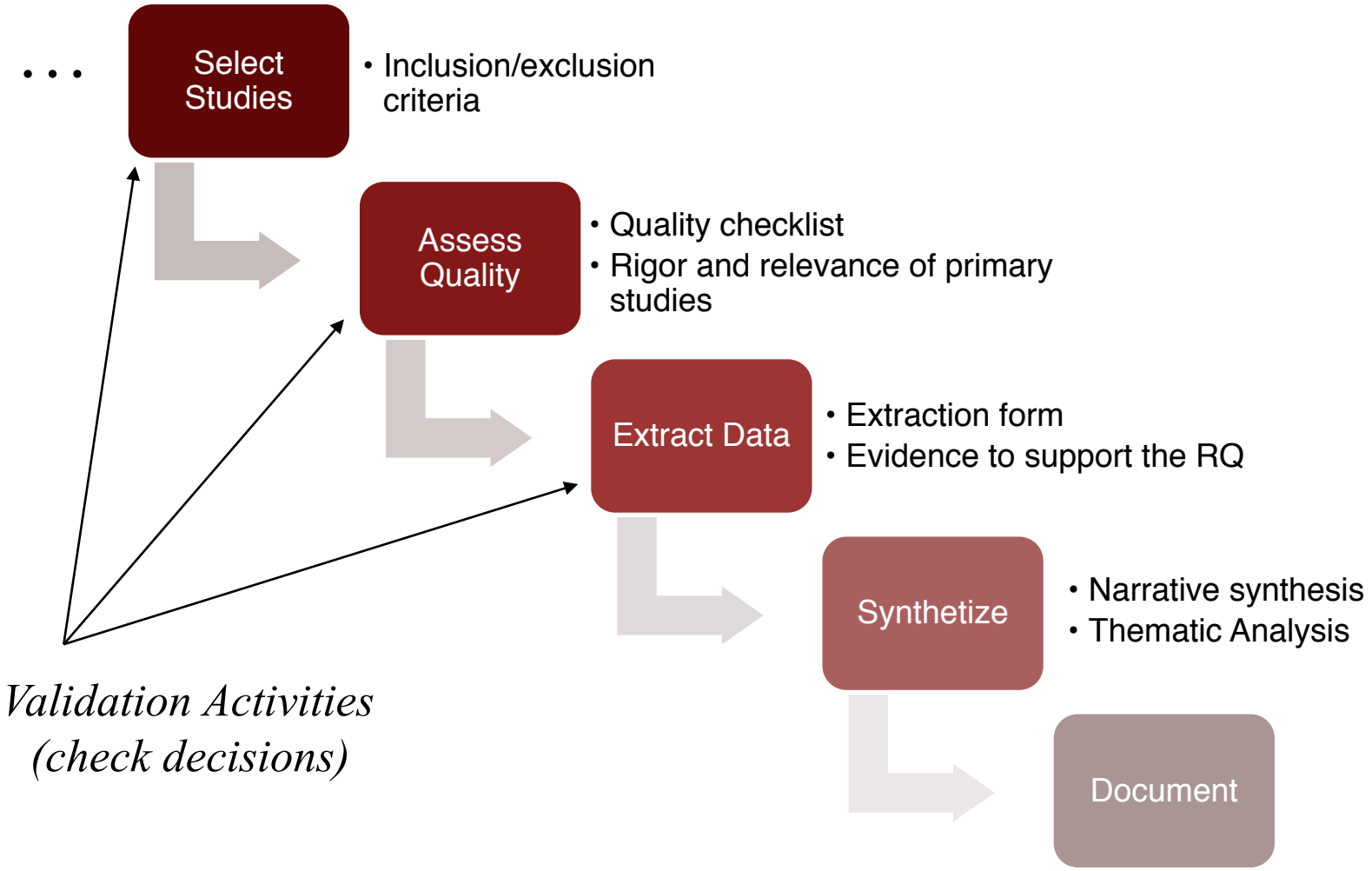


Source: Zhang, H., Babar, M.A., Tell, P.: Identifying relevant studies in software engineering (adapted).

Primary Study Selection

Inclusion Criteria	Exclusion Criteria
• research related to estimation/measuring the effort or cost of security in software development • research on software security and presents effort/cost results • published between 2000 up to and including 2017	• reactive approach to software security issues • research about software safety • not presented in English • not accessible in full-text • book or gray literature • tutorial, workshop or poster summary • study is duplicated

Next Steps in the Systematic Review



References

- Boehm, B. Software Engineering Economics, Prentice-Hall, Upper Saddle River NJ (1981).
- Hahn, R.W., Layne-Farrar, A.: The Law and Economics of Software Security. Harvard Journal of Law and Public Policy; Cambridge. 30, 283–353 (2006).
- Heitzenrater, C., Simpson, A.: A Case for the Economics of Secure Software Development. In: Proceedings of the 2016 New Security Paradigms Workshop. pp. 92–105. ACM, New York, NY, USA (2016).
- Kitchenham, B.A., Budgen, D., Brereton, P.: Evidence-Based Software Engineering and Systematic Reviews. Chapman and Hall/CRC, Boca Raton (2015).
- McGraw, G.: Software security. IEEE Security Privacy. 2, 80–83 (2004).
- McGraw, G.: Cyber War is Inevitable (Unless We Build Security In). Journal of Strategic Studies. 36, 109–119 (2013).
- Zhang, H., Babar, M.A., Tell, P.: Identifying relevant studies in software engineering. Information and Software Technology. 53, 625–637 (2011).
- Yang, Y., Du, J., Wang, Q.: Shaping the Effort of Developing Secure Software. Procedia Computer Science. 44, 609–618 (2015).