DB Systel
Digital.
Empowered.

The Burden of Knowledge

Dealing With Risks in Open Source

DB Systel GmbH | CTO Team | Max Mehl | FOSS Backstage | 10.03.2025

Our Journey

1. From Assumptions to Data
2. Metrics Are Not Easy
3. Available Options for Risk Management
4. Recommendations, Outlook, Discussion

Houston, Someone Mentioned There Might Be a Potential Issue

Assumption about Open Source usage

- 5-7 digit number of third-party packages
- Direct and indirect dependencies
- Spread over 3-5 digit number of internal projects

We need data!

Knowledge about Open Source risks

- Security vulnerabilities
- License changes towards proprietary
- Sustainability issues, e.g. low/no maintenance

CISA Framework for Measuring Trustworthiness

> The task of assessing the trustworthiness of OSS [...] is **more complex for OSS** than for proprietary software, because there is, generally speaking, **no direct relationship** between the authors of software and those who use that software.

> Even when mature open source software projects publish software bills of material or other artifacts of secure software development practices, it is the **responsibility of those who use the project** to perform the necessary diligence to continually assess **each open source project**."

"The number of active contributors, or unexpected changes in account ownership"

"The presence of known vulnerabilities or out-of-date dependencies"

"Whether the project requires two-factor authentication on developer accounts"

"Whether the project requires code review, or has a responsible vulnerability disclosure process"

Source: https://www.cisa.gov/news-events/news/continued-progress-towards-secure-open-source-ecosystem

Passive Metrics Are Not Sufficient to Manage Open Source Risks

Most metrics typically only measure what can be easily measured

- Hot take: They cannot replace an experienced „gut feeling“ about project

Bad scores do not seem to correlate well with materialised risks

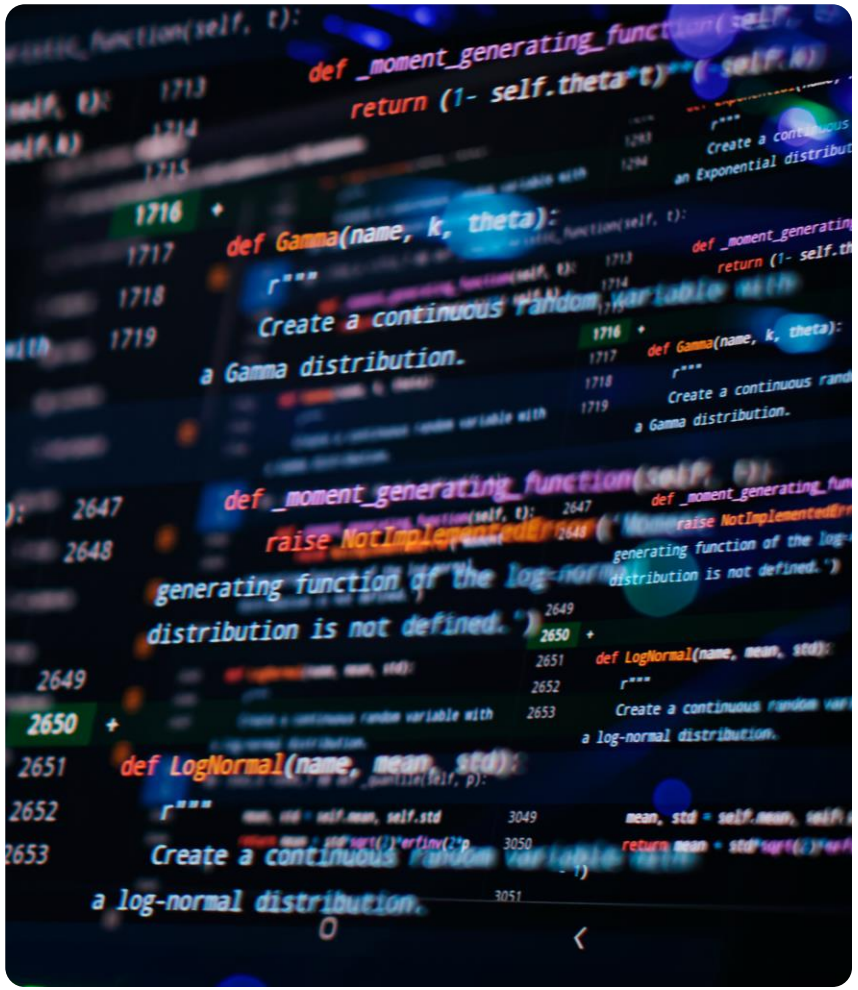
- Study: OpenSSF Scorecard scores only explains 12% of vulnerabilities. Other factors matter more[1]

Therefore, many factors that define quality and risk are often disregarded

- Examples: Behaviour of maintainer, connection to a foundation, driven by only one company we do (not) trust (“single-vendor project”)
- CHAOSS covers some of these indicators, but it does not weigh them

Most importantly, passive metrics do not make us actionable

- A bad rating alone does not provide any decision path
- They do not provide alternatives. Often, there is only one economic solution
- Most often, the usage of badly rated projects are not in our control → use as indirect dependencies



1: Source: https://arxiv.org/abs/2210.14884

Case Study: Challenges of Open Source Usage and Potential Risks at Deutsche Bahn from a Quantitative Point of View

32.300 internal repositories and their SBOMs analysed (code, config, documentation)

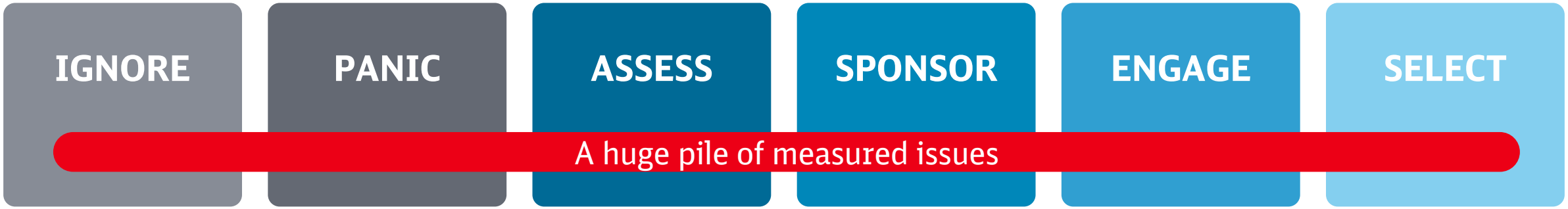
125 dependencies on average per internal project

117.000 packages in use, most of them Open Source

19% of internal projects contain the most-used dependency

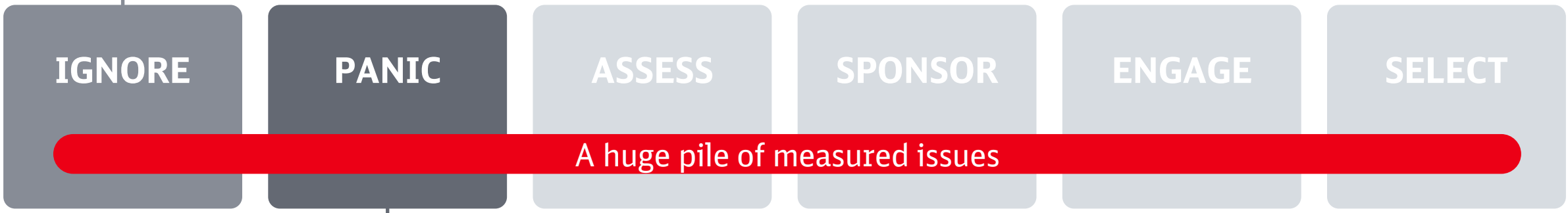
9/10 most used dependencies score < 5/10 on OpenSSF Scorecard

Which Options Do We Have to Mitigate Risks in Open Source?



Available Options 1/3: IGNORE and PANIC

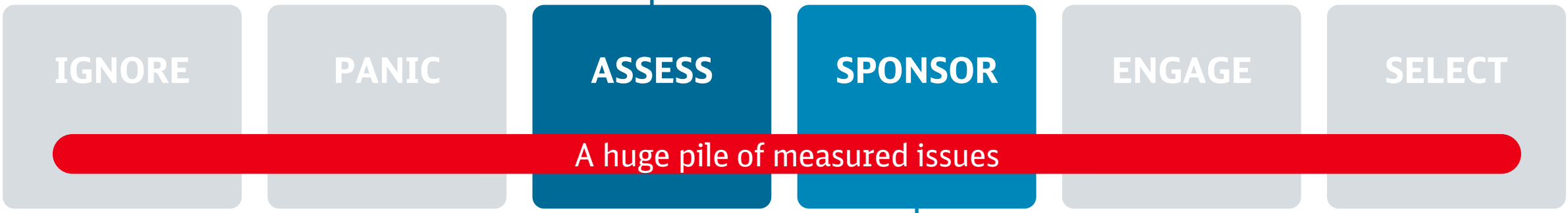
- A lot of data can be overwhelming
- Especially if it indicates many issues that cannot be mitigated easily
- Hide or play down issues as they could scare off management, and destroy the reputation of Open Source in an organisation



- Forbid usage of all software with bad metrics
- Replace affected dependencies with software that has better metrics
- Contact maintainers of affected projects, demand them to fix issues, ask them to fill out forms

Available Options 2/3: ASSESS and SPONSOR

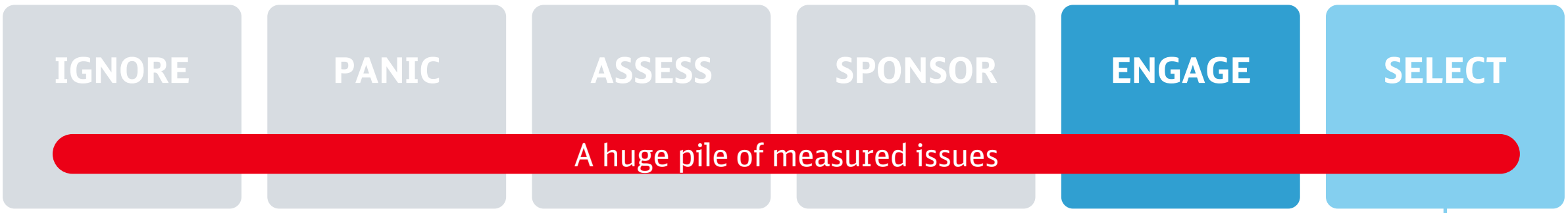
- Identify your own risk profile: “What is actually important for me?”
- Identify which qualitative and quantitative properties of Open Source projects make a difference
- Group your assets into risk classes to prioritise efforts



- Support Open Source projects financially on your own
- Fund projects indirectly by Sovereign Tech Agency programmes or Tidelift
- Nudge foundations you are member of to support certain projects

Available Options 3/3: ENGAGE and SELECT

- Become (co-)maintainer of projects important to you
- Set up internal teams that provide support and coordinate contributions
- Partner with like-minded organisations to share efforts



- Prevent use of problematic Open Source projects proactively
- Enable your teams to make wise selections of projects, by criteria based on your individual risk assessments
- Metrics and tools may assist the teams with their selection

Good Example: US White House Cybersecurity Priorities (2024)

Improve Open Source Software Security and Sustainability

Recognizing the many benefits of open source software, departments and agencies should ensure secure use of open source software and **contribute to maintaining open source code** to help sustain components depended on by the agency.

Maintenance activities could include developing mechanisms that **enable and encourage employees and contractors** to contribute to open source software components, including security-related contributions; monitoring changes to code; tracking and correcting potential errors and flaws in code; and other related activities.

Agencies **should integrate open source software considerations**, including processes to review, approve, inventory, and centralize open source consumption, into agency IT and cybersecurity governance structures.

Agencies are encouraged to **study the benefits** that can be gained through establishment of a governance function modeled after private sector open source program offices that **define roles, responsibilities, and methods of engagement**.

Source: https://www.whitehouse.gov/wp-content/uploads/2024/07/FY26-Cybersecurity-Priorities-Memo_Signed.pdf

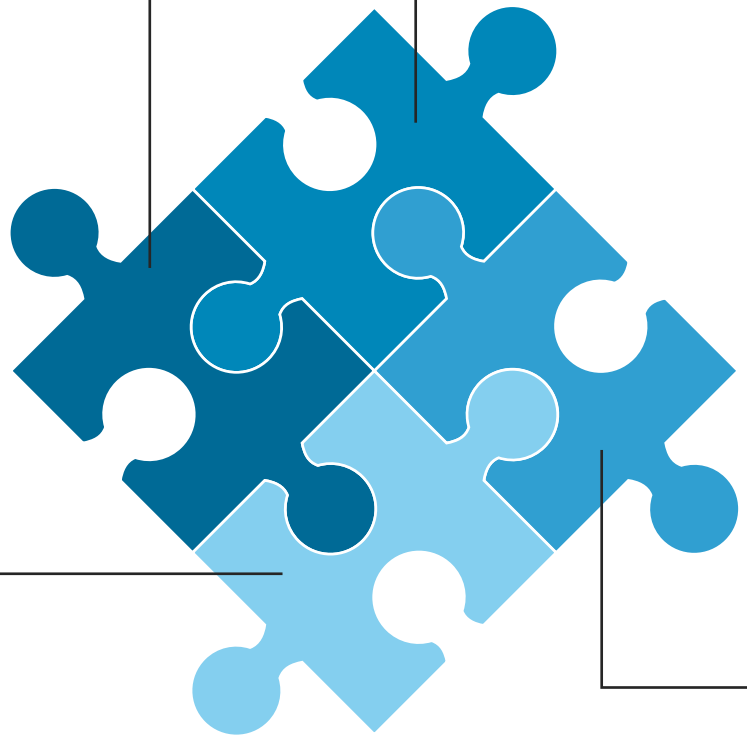
Conclusion: Recommended Toolbox

ASSESS

Identify which (un-)measurable factors matter for you and your risk profile(s)

SPONSOR

Support projects important to you and their maintainers financially



SELECT

Enable your teams to choose Open Source projects wisely, avoid problems proactively

ENGAGE

Participate in Open Source projects that are critical to you

What‘s to Be Done? How Can We Collaborate?

Collaborate to reduce duplicated work!

Share Open Source project assessments
and criteria, especially qualitative.

Get active!
Time‘s over for passive consumption.

Thank you!

Contact

Max Mehl
Open Source Governance & Strategy

max.mehl@deutschebahn.com

@mxmehl@mastodon.social

@mxmehl