escrypt
SECURITY. TRUST. SUCCESS.

In cooperation with
KPMG

Whitepaper

Automotive Cyber Maturity Report 2022

PROOF

Contents

Executive summary

Automotive cybersecurity is rapidly evolving due to disruptive trends such as automated driving, vehicle cloud computing, and increasing regulation. Managers across all levels of the organization must navigate this ocean of cybersecurity requirements. This 2022 edition of ESCRYPT and KPMG's annual cyber maturity survey provides a compass: Facts and figures on the industry's current cyber maturity, progress and developments since last year, as well as trends and remaining open challenges. The demand for this information is high and backed up by the industry's response to our survey. This year saw more than 280 participants from over 160 automotive companies, a tremendous fourfold increase over the previous year.

Our survey results show that a small elite of manufacturers and suppliers lead the way while the vast majority has just embarked on their mission to secure road users, customers, and business models (see Figure). We distilled four key takeaways from all responses:

- Takeaway #1: Mature organizations think and act differently: Mature organizations tackle cybersecurity end-to-end across the whole product life cycle with a DevSecOps mentality whereas organizations in initial stages of their implementations have a limited scope mostly focusing on development aspects. Higher maturity comes along with increased satisfaction of cybersecurity status and progress.
- Takeaway #2: Cyber talent shortage persists: Competencies and sufficient capacities stay the major concern (see also survey 2021) across all organizations independent from their maturity level.
- Takeaway #3: Budgeting for cybersecurity: Budgeting is a major challenge for almost 50% of the respondents. While established maturity organizations see stable or even increased budgets, organizations at initial stages often lack fixed budgets or budgets are even unknown.
- Takeaway #4: End-to-end security is a hallmark of cyber maturity: Cyber mature organizations understand that automotive security must be defended along three crucial dimensions: Securing (i) the ecosystem, (ii) the supply chain, and (iii) the lifecycle.

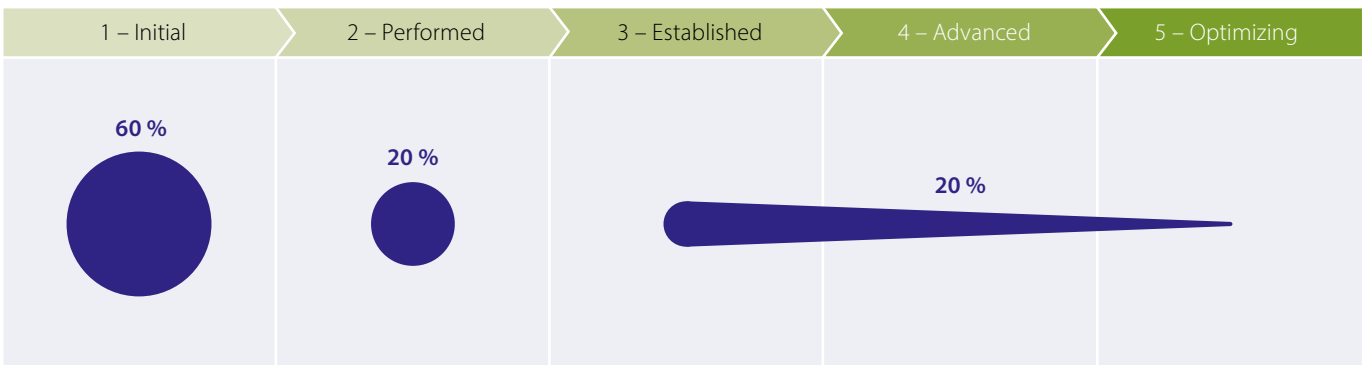


Figure 1: Self-assessed cyber maturity of over 160 automotive companies.

Context and objective of this year's survey

Four technological disruptions - automated driving, connectivity, electrification, and new mobility use cases - have become central topics in the automotive industry. Each disruption increases the relevance cybersecurity plays in this transformative era. In fact, software vulnerabilities have already led to safety recalls, automotive-specific regulations such as the UN Regulation 155 and the development of the GB and GB/Ts in China mandate security in the largest markets, and the majority of manufacturing and automotive companies recently ranked cyber incidents as a top 5 business risk in the Allianz Risk Barometer 2022.

Since our cyber maturity survey in 2021, the ISO/SAE 21434 has been published as international standard and the first automotive manufacturers and suppliers have had their CSMS certified according to UN R 155 respectively ISO/SAE 21434. All the while the maturity of the industry as a whole is rapidly developing in many companies through internal projects as well as horizontal collaboration in forums such as the Auto-ISAC and its regional counterparts. So, at the beginning of this year, it was time for an updated survey.

The objective of our annual survey remains the same: To determine the current state of automotive cyber maturity, identify trends and challenges, and derive paths forward for manufacturers, suppliers, and the industry. Automobiles and business models are changing fast, and so must the necessary and required cyber protections. This report provides facts and figures for leaders in automotive companies to progress with speed and focused actions towards higher maturity.

We are excited to see a fourfold increase in participation in this year's survey – a clear sign that this report is needed and provides value. This year we asked participants to self-assess the maturity of their cybersecurity management system on a scale from initial via established to optimizing (see textbox "PROOF automotive cyber maturity model" for details). This allowed us to separate responses from different maturity levels and led to striking insights: Highly mature organizations think and act differently in multiple crucial ways. We thank all participants of this survey for their time and responses and are happy now to share the full results and key takeaways with everyone in this year's ESCRYPT & KPMG's automotive cyber maturity report.

PROOF automotive cyber maturity model

5 – Optimizing
4 – Advanced
3 – Established
2 – Performed
1 – Initial

PROOF is short for product security organization framework. It is a maturity model for assessing the status of cybersecurity at automotive companies. PROOF consists of over 120 automotive security specific controls that rate the maturity on five levels from "initial" via "established" (implying an organization that performs cybersecurity activities in a repeatable, formalized fashion) to "optimizing" (implying an organization that actively and continuously improves its cybersecurity activities in a structured way).

PROOF is standards-based

- Based on the ISO 3000 series like ASPICE
- Uses five maturity levels like CMMI
- Developed by ETAS and KPMG leveraging decades of experience

PROOF is built for automotive

- Considers international automotive security regulations & standards such as UN R 155 and ISO/SAE 21434
- Integrates national frameworks from China, the US, Europe, and Japan such as NHTSA and JasPar.
- Used by automotive manufacturers and suppliers from China, Europe, Japan, and other regions.

2022 survey design and statistics

Participation increased fourfold compared to 2021

- Timeframe: February – April 2022
- Scope: Open to automotive companies worldwide
- Style: Twenty multiple choice questions (self-assessment)

Part 1: Governance
The survey is organized in four parts with five questions each. The first part "Governance" deals with the "who" and "what" of cybersecurity activities at automotive manufacturers and suppliers: Who heads the initiatives and what is in scope.

Part 2: Progress and Challenges
The second part "Progress & challenges" focuses on "how" and "which": How mature are the organizations and what challenges do they face.

Part 3: Risk Management & Supply Chain Management
The third part zooms in to "Risk management & supply chain management" topics. This includes the question of most concerning attack vectors and how cyber maturity in the supply chain develops.

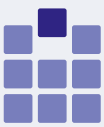
Part 4: Product Lifecycle
The final part "Product lifecycle" assesses how the participants manage cybersecurity beyond initial development until their products' end of life. In combination, the answers to the four parts allow key insights into the automotive industry's current cyber maturity and identify directions how to progress further.

280+ respondents
up more than 4x from last year

160+ companies
up to 28 responses per company*

* To achieve more balanced statistics, the report aggregates responses from same company and country

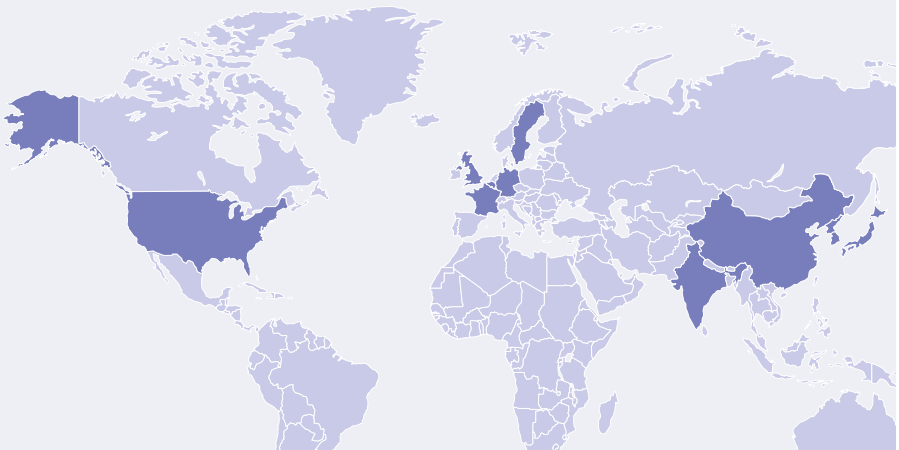
13% OEM



87% Supplier

Participants come from ten countries including all top 5 automotive markets:
China, France, Germany, India, Italy, Japan, Korea, Sweden, United Kingdom, US

Participants: Managing directors, chief information/product security officers (CISO/CPSO), department heads, managers, security managers and specialists, quality managers, engineers and developers



The ratio of participating suppliers has increased compared to last year. This reflects that the transformation process toward higher cyber maturity has reached the supply chain.

Key takeaways

Four main takeways lead the way to increased automotive cyber maturity

Takeaway #1: Mature organizations think and act differently

The first takeaway is our main insight: Mature organizations think about cybersecurity and mitigate cyber risks very differently from less mature ones (cf. Question 6). The survey data paint a striking picture: Increasing cyber maturity is correlated with increasing satisfaction about progress with the cybersecurity management system (see Figure 2), with increasing cybersecurity budgets (see also Takeway #3) and an increasing end-to-end coverage of security and DevSecOps mentality (see also Takeway #4). More mature companies have a clearer understanding of what they need to master cyber threats and thus can and do take more decisive and ultimately successful steps in protecting their products and customers. It is not that the issues considered at initial maturity (often R&D centered) become irrelevant, but rather that at established maturity additional topics complement and enhance the cybersecurity approach such as closer links between product security and classical information security (see also Figure 3).

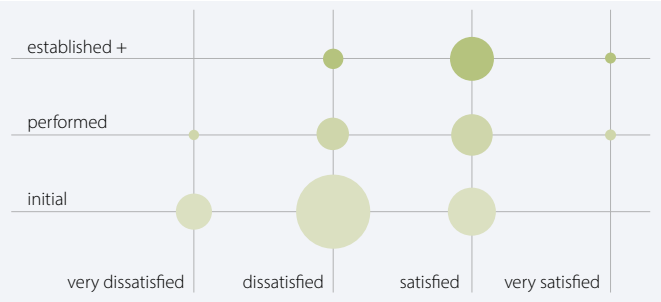


Figure 2: More mature organizations are more satisfied with their progress

Initial maturity organizations	Established+ maturity organizations
R&D is head of CSMS	**IT** is head of CSMS
Frameworks considered most relevant for CSMS: **ISO 26262, ISO/SAE 21434, UN R 155**	Frameworks considered most relevant for CSMS: **ISO/SAE 21434, UN R 155, ISO 27001**

Figure 3: From safety and R&D to holistic integrated security management systems

Takeaway #2: Cyber talent shortage persists

Competence and sufficient capacities were the major concern for automotive companies in our 2021 survey (65% vs. 42% of the votes for the runners-up concern). This trend manifests itself in this year's results: Competences and capacity are the most and second-most voted-for challenges (cf. Question 9). In fact, (lack of sufficient) competencies are the prime challenge in all domains of a cybersecurity management system (see Figure 4). The only exception is the risk management domain which is already a relatively well-developed part of many CSMSs (cf. Question 11). Interestingly, the talent shortage is a challenge for initial and established maturity companies alike. Almost half of both voted for competencies.

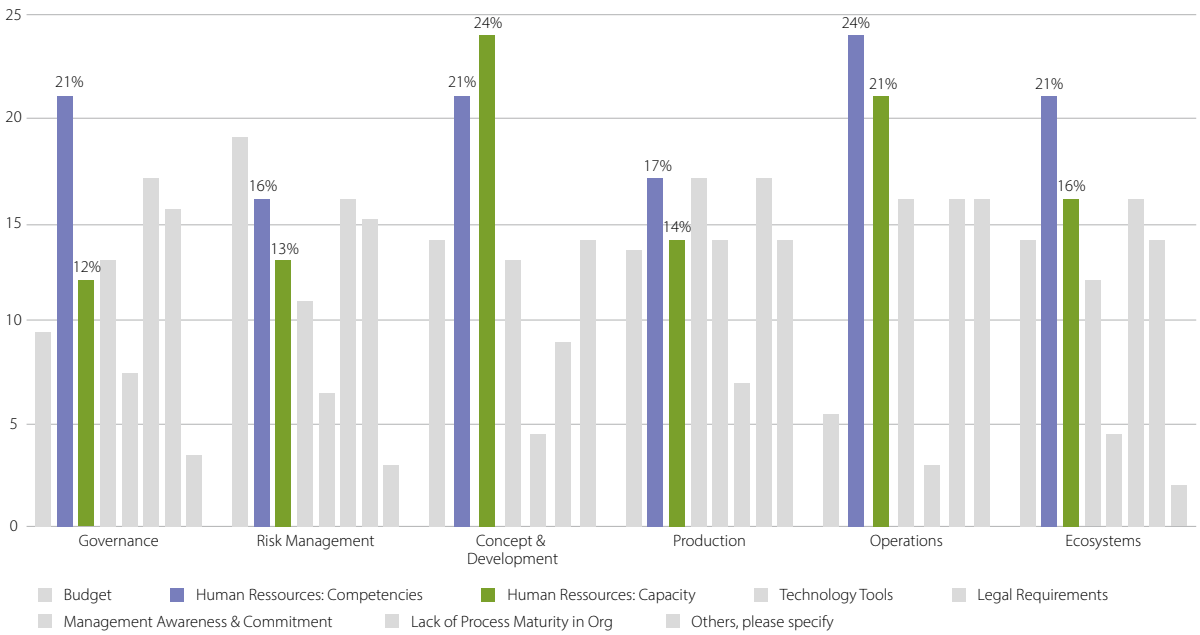


Figure 4: Top challenges in each CSMS domain

Takeaway #3: Budgeting for cybersecurity

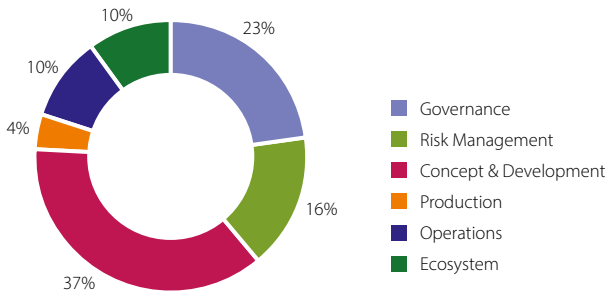
Another frequently selected challenge for cybersecurity was budgets. While almost half of respondents reported stable or increased budgets, a staggering 46% did not have a clear picture of their cybersecurity budgets at the time of the survey in the first quarter of this year (cf. Question 10). The difference between initial maturity and established maturity organizations couldn't be starker: Most of the former said budgets are still not fixed or known while the majority of the latter stated an increase. Consequently, budgets are three times more likely to be selected as a challenge at initial maturity (cf. Question 9).

Budgets 3x more likely a challenge at initial maturity

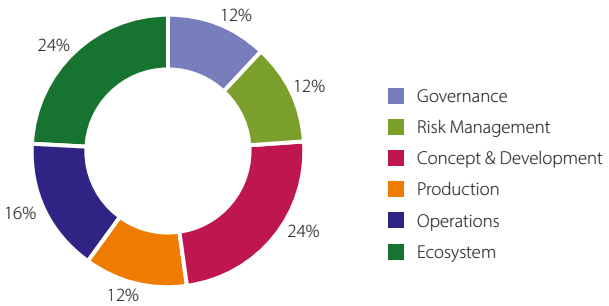
This aligns with our observations as automotive security consultancy. Companies that start out in their product security journey often take small, probing steps to learn and avoid bad investments. In contrast, high cyber maturity companies have a clear understanding of the necessary security measures on both a technological and organizational level. They can (and do) make informed decisions on the right investments.

CSMS domain with the biggest challenges

Initial maturity organizations



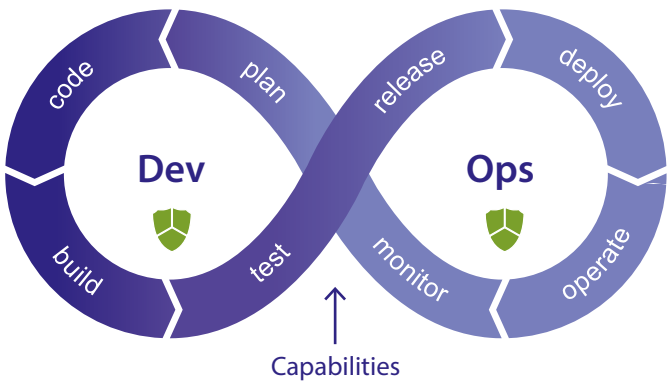
Established+ maturity organizations



Takeaway #4: End-to-end security is a hallmark of cyber maturity

Cyber mature organizations understand that automotive security must be defended along three crucial dimensions: First, the ecosystem dimension. Attacks can launch from many different parts of the automotive ecosystem. Respondents from established maturity manufacturers and suppliers recognize this and significantly more often are concerned about attack vectors targeting workshops, backend systems, production, and the supply chain (cf. Question 13). This leads to the second dimension, the supply chain. At initial maturity none of the respondents were satisfied with their supply chain maturity while one in five did not know about their supply chain maturity. At established maturity satisfaction increases to a quarter while the uncertainty drops to one in twelve (cf. Question 14). Finally, highly mature organizations understand that security must be established and maintained for the entire product lifecycle while the focus at initial maturity is on pre-SOP activities (cf. Question 8).

This is then the hallmark of cyber maturity: Securing the ecosystem, the supply chain, and the lifecycle. DevSecOps will play a crucial role to achieve protection along all three dimensions. It augments the DevOps cycle with security relevant capabilities. We already see an eightfold increase in DevSecOps adoptions among participants as we move from initial maturity to high maturity companies (Question 16). We explore these topics in greater detail in our forthcoming whitepaper on the cybersecurity for the software-defined vehicle.



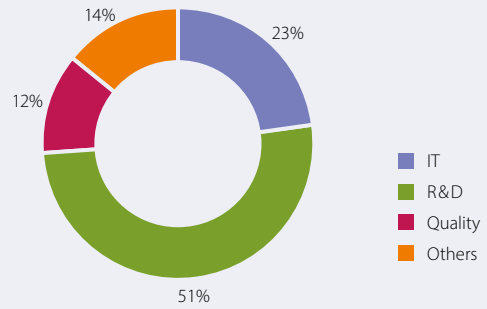
+ Dependency tracking
+ Continuous monitoring
+ Continuous risk assessment
+ Code Signing
+ Dynamic code analysis
+ Information sharing
+ Patching SLAs
+ …

Survey results in detail

Governance

1) Which departments heads your organization's CSMS?

(Single answer)



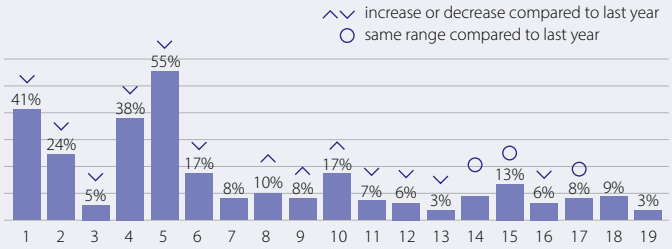
R&D natural choice for most participants as head of CSMS since it directly impacts how products are developed.

Interesting: many companies have created dedicated departments/ teams ("others"), e.g.:

- Security Committee, Security Department
- Quality+ R&D + IT (Combination)
- Team Cybersecurity
- Business Management, Management Support Team
- Technical Compliance, QM-ISO Promotion Department
- Verification Team, Planning Team

2) Which frameworks are most relevant for the product security activities in your area of responsibility?

(Multiple answers)



1 UN R 155 (CSMS)
2 UN R 156 (SUMS)
3 UN R 157 (ALKS)
4 ISO/SAE 21434
5 ISO 26262
6 ISO 27001
7 ISO 24089
8 ISO 22301
9 IEC 62443
10 VDA ASPICE for Cybersecurity
11 VDA ACSMS Red Volume
12 GDPR
13 EU NIS Directive
14 NHTSA Cybersecurity Best Practices
15 NIST Cybersecurity Framework
16 Jaspar Cyber Security Quality Assurance Guide
17 China's ICV Market Access Guide and related GB& GB/T standards
18 Do not know
19 Other, Please Specify

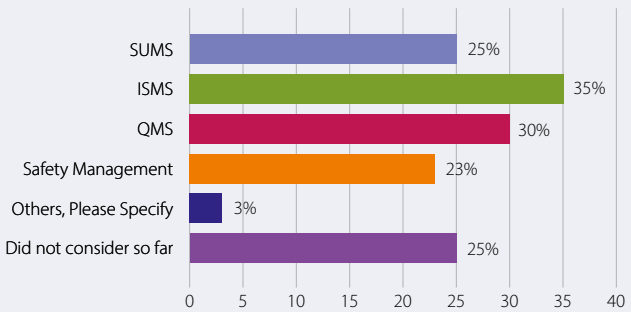
Regulations UN R 155, 156 and Standards ISO/SAE 21434, ISO 26262 remains the same in top four slots compared to last year. Results show that still safety and security are closely pinned together.

VDA ASPICE for cybersecurity grew in relevance.

Key observation: Response rate for China's ICV far lower than our experience from direct client discussion.

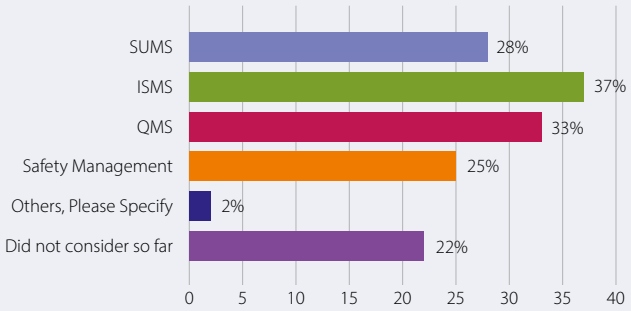
3) Which of the following management systems does your organization integrate with its CSMS into one management system?

(Multiple answers)



4) For which of the following management systems has your organization established interfaces (but no full integration) with its CSMS?

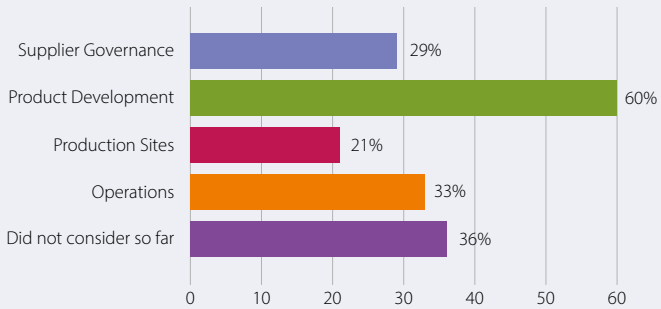
(Multiple answers)



We see a convergence of information security and product security as CSMS is often integrated with ISMS.

5) Which of the following areas are already integrated in your organization's CSMS?

(Multiple answers)



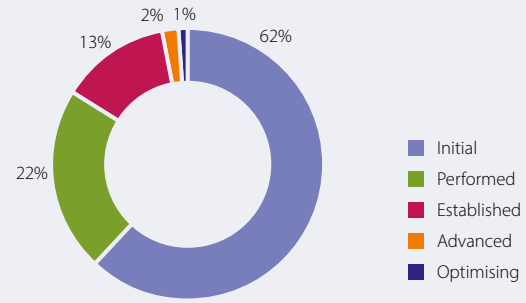
This supports the results from the first question in which most participants selected R&D as their head of CSMS.

Remark: A CSMS is most effective when it manages security end-to-end. So, more focus should be built upon other areas too.

Progress & challenges

6) How do you rate the overall maturity of your organization's CSMS?

(Single answer)

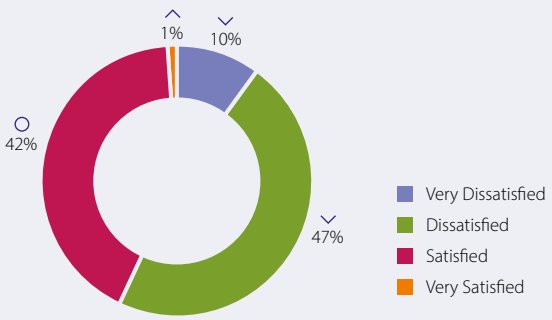


Almost one fifth have an established CSMS and are thus expected to pass for certification. More than a third at least perform cyber-security management which is highly promising in terms of industry maturity.

However: most companies are still in the initial stages of the transformation toward a full CSMS.

7) How satisfied are you with the progress regarding CSMS in your area of responsibility since last year?

(Single answer)

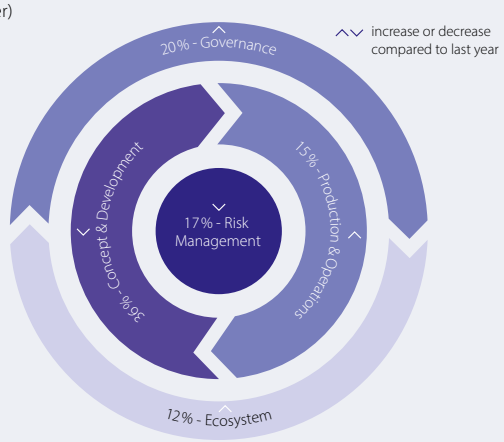


Plain comparison: Same relative numbers, but in absolute numbers: many more companies are satisfied

Results seem highly correlated with previous question: around 60% at initial stage of CSMS and similar level is (very) dissatisfied.

8) Which is in your view currently the domain with the biggest challenges?

(single answer)



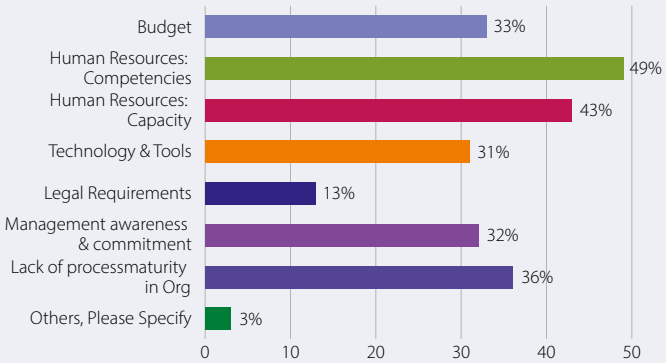
Majority still perceives concept & development as domain with biggest challenges.

Governance and not risk management now second most frequently selected domain with biggest challenges.

Overall, votes are more evenly spread and challenges in other domains increasingly come into spotlight.

9) What kinds of challenges do you face in this domain?

(Multiple answers)



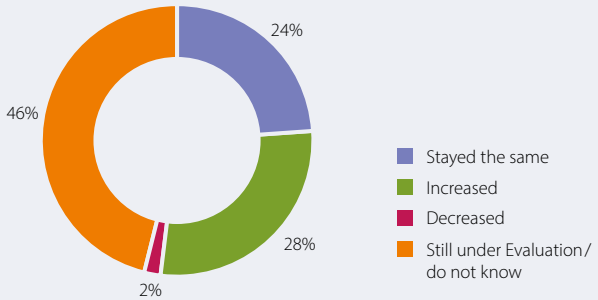
Both sufficient talent and competencies are the most selected challenges. As everyone is building up their CSMS, this is to be expected. While we expect the pressure to ease somewhat, it will remain high for the foreseeable future.

Lack of process maturity unsurprising since most participants do not yet have an established CSMS.

Challenges with management awareness and commitment should be solved with high priority.

10) How has the budget for the CSMS implementation in your area of responsibility developed compared to last year?

(Single answer)



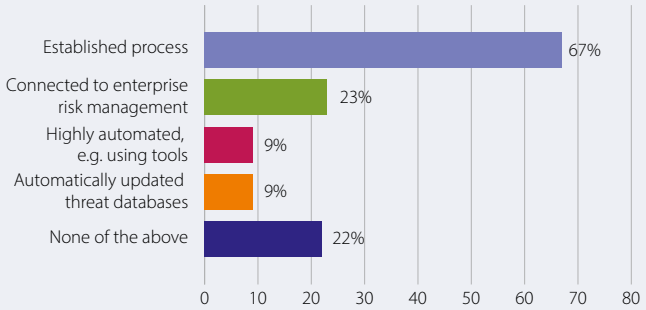
Positive: more than a quarter saw budget increases, hardly anyone budget cuts.

Attention needs to be paid to the large percentage of "still under evaluation".

Risk management & supply chain management

11) How does your organization's CSMS implement risk management?

(Multiple answers)

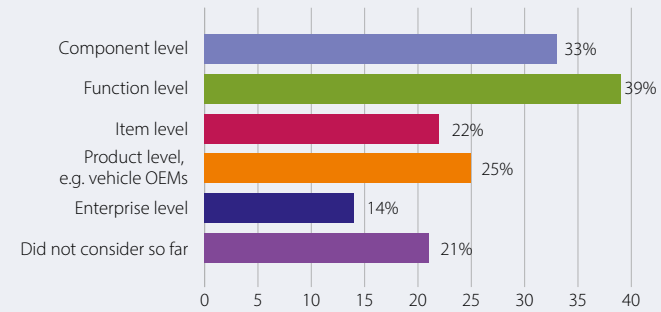


Even though almost 2/3 of participants rated their CSMS maturity as "initial", 2/3 have established risk management processes: Risk management is the heart of a CSMS!

Few organizations (yet) seem to implement higher efficient/automated approaches. This will be a main driver for new solutions in the next years.

12) On what levels does your organization's CSMS perform risk management?

(Multiple answers)

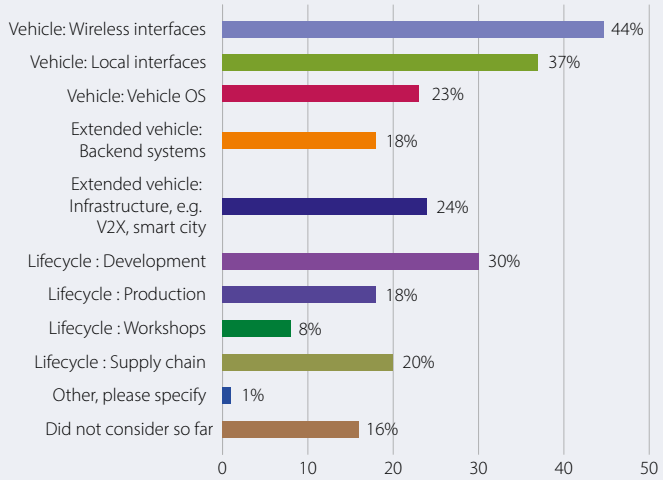


Risk management on multiple levels still a field of growing maturity. Percentages for product and item level seem surprisingly low considering requirements from UN R 155 and ISO/SAE 21434.

Enterprise level risk management will set holistic acting organizations apart from more siloed organizations. This means end-to-end risk management covering IT, OT, cyber, and other areas.

13) What attack vectors are you most concerned about?

(Multiple answers)

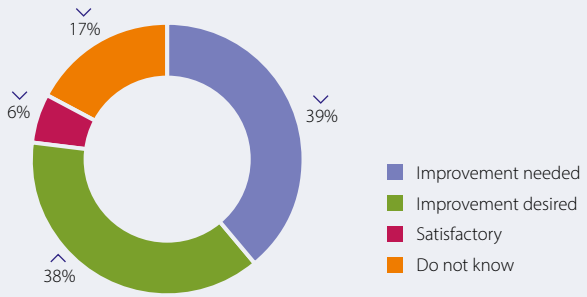


Wireless interfaces unsurprisingly lead on top.

Extended vehicle, production, supply chain need more attention because attacks here have the potential to scale.

14) How do you rate the cyber security maturity in your organization's supply chain?

(Single answer)

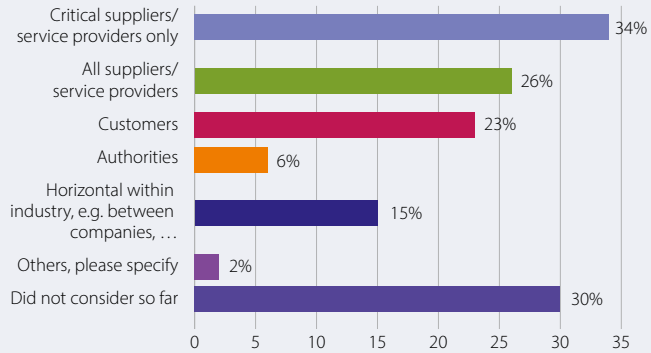


Very encouraging: Even though we had many new survey participants this year, most of which are at initial maturity of their CSMS, both "unknown" and "improvement needed" shrank compared to last year

However: Supply chain maturity is still a big topic. Slightly more than last year selected improvement needed/desired (cf. also Question 5).

15) What scope does your organization's CSMS ecosystem management have?

(Multiple answers)



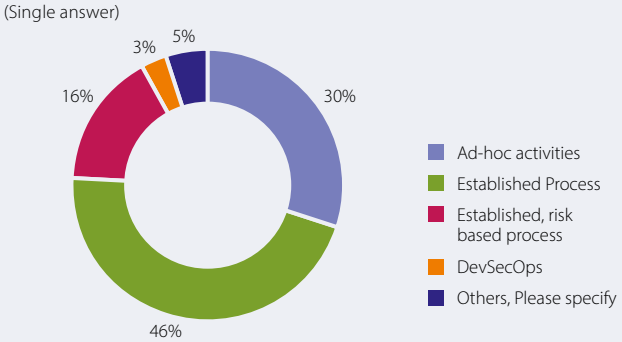
30% "did not consider ecosystem" in line with the initial maturity of most CSMS of participants but must be resolved before a full CSMS is reached.

We encourage more horizontal activities, e.g., in forums like Auto-ISAC.

Product lifecycle

16) How does your organization's CSMS implement security activities during concept & development?

(Single answer)

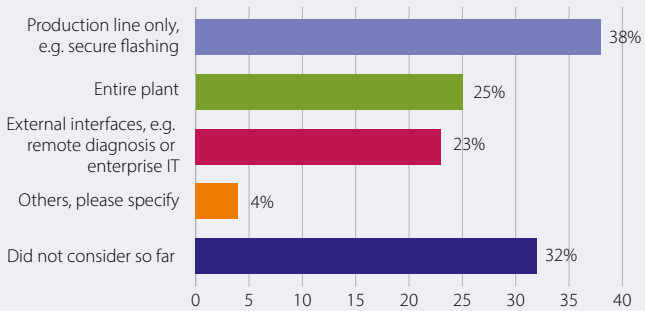


2/3 have established process within concept & development domain in line with R&D as head of CSMS of most participants (cf. Question 1).

1/5 have more advanced processes, e.g., risk-based and DevSecOps. This maturity will set companies apart from competition and enable them to secure product over the entire lifetime.

17) What is in the scope of your organization's CSMS in the production domain?

(Multiple answers)

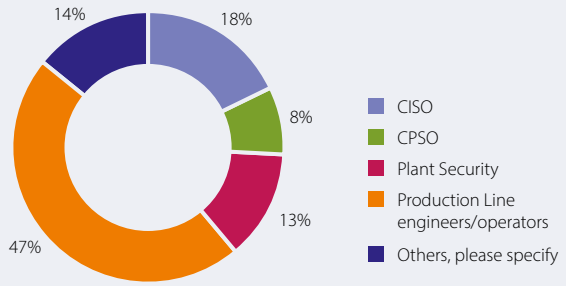


Secure production line first good step but take note of recommendation in ISO/SAE 21434 to implement IEC 62443.

Almost a third did not consider production yet (cf. also Question 5).

18) Who in your organization is responsible for the CSMS in the production domain?

(Single Answer)



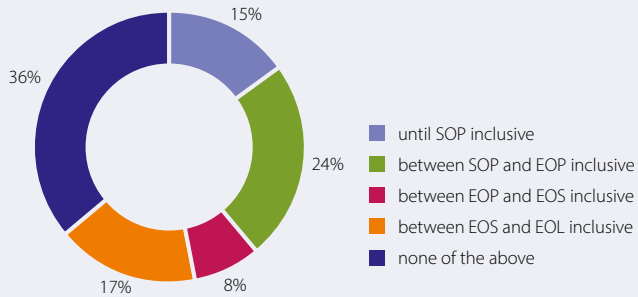
Production level Engineers are heading the CSMS in Production domain.

Traditional CISO approach comes next.

Joint forum/interface with CPSO should be established to ensure product security and OT security are aligned in case CPSO does not lead it.

19) How long is your organization's CSMS prepared to support security of a given product?

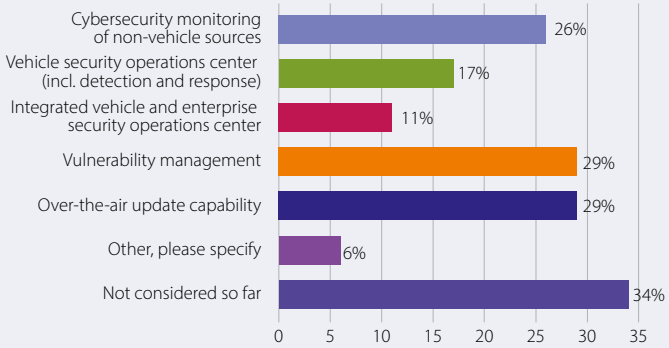
(Single answer)



It should be the aspiration to support product security all the way until end of life in line with a company's quality objectives and promise to the customer.

20) What aspects of security operation has your organization's CSMS already established?

(Multiple answers)



Automotive companies implement many different aspects for security operation, but none individual aspect (yet) used by majority.

Interesting to note: All measures (combining both VSOC answers) score about the same. Might be an indication that some companies implement many measures and others none.

Contacts

Dr. Moritz Minzlaff
Head of Professional Security Services
ETAS GmbH
moritz.minzlaff@etas.com

ETAS GmbH
Borsigstraße 24
70469 Stuttgart, Germany
+49 (234) 43870-200

www.escrypt.com
www.etas.com

Jan Stölting
Partner Cyber Security
jstoelting@kpmg.com

Hans-Peter Fischer
Partner Cyber Security
hpfischer@kpmg.com

KPMG AG Wirtschaftsprüfungsgesellschaft
THE SQUAIRE
60549 Frankfurt, Germany
Telephone: +49 69 9587-0

www.kpmg.com
www.kpmg.com/socialmedia

Acknowledgements

Martin Delle, Veronika Klein, Michael Klinger, Bianca Knittel, Jungseo Park, Sabari Pasupathi, Matar Rami, and many more

Last updated: 12/2022