MHP
A PORSCHE COMPANY

zentrum Nachhaltige Transformation
an der Quadriga Hochschule Berlin

STUDY

Ready to Defend?

How Well Germany's Mid-Market Companies Manage Their Resilience

AI

Berlin, October 2026

A study by MHP Management and IT Consulting and the Center for Sustainable Transformation (zNT) at Quadriga University Berlin

MHP
A PORSCHE COMPANY

zentrum Nachhaltige Transformation
an der Quadriga Hochschule Berlin

Germany's mid-market companies (often referred to as the Mittelstand), defined here as companies with annual revenue of up to €5 billion, employ around 80 percent of the country's workforce and generate approximately two-thirds of its GDP. These companies are a pillar of the German economy, but they face a difficult position. Many consider themselves too small to invest in dedicated management resources for defense preparedness, yet they are too large and too deeply embedded in supply chains to simply ride out the effects of crises and conflicts.

For this study, polling firm Civey surveyed 1,000 managers at companies with annual revenue between €50 million and €5 billion. The survey was conducted from July 31 to August 17, 2026.

Executive Summary

Germany's security environment has deteriorated. Alongside military threats, hybrid threats such as espionage, sabotage, disinformation, and foreign interference increasingly shape the risk landscape. For companies, this means that supplies, supply chains, employees, and day-to-day operations may all face serious disruption. This applies even to businesses outside the critical infrastructure sectors. Companies must also be prepared to assume responsibility for security and defense beyond their own operations and recognize their role in Germany's national preparedness.

Germany's mid-market companies are willing to take responsibility:

79%

see crisis resilience and defense preparedness as increasingly important to their industry.

86%

would be willing to make capacity available for national defense.

93%

consider their industry relevant to security of supply.

There is, however, a substantial gap between recognizing this responsibility and being able to contribute in a crisis or defense scenario. The challenge is to turn willingness into operational capabilities. This calls for Defense Readiness Management that determines what role each company would play, what it could deliver, how quickly it could respond, how long it could sustain its contribution, and which supply chains, energy sources, personnel, and IT systems it depends on.

Five Capabilities Underpin Defense Readiness

The objective of this management approach is Defense Readiness: the ability of a company to remain operational during a crisis while making a reliable contribution to security of supply and national defense. Defense Readiness rests on five essential capabilities (Figure 1):

1. understanding the company's role within the national security context
2. identifying and understanding risks
3. assessing threats and vulnerabilities across its supply chains
4. establishing business continuity management, including contingency options and emergency plans
5. strengthening cyber resilience

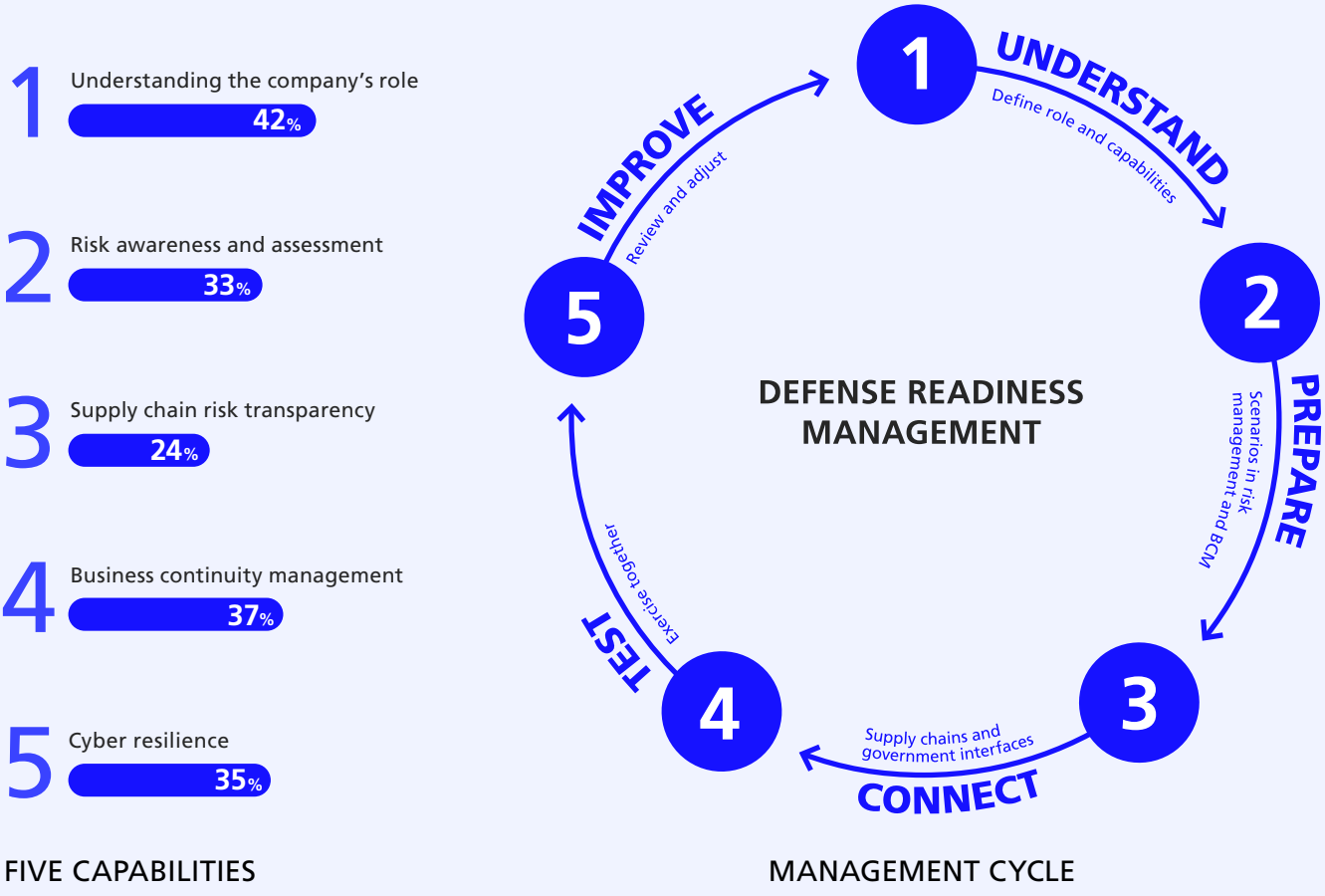


Figure 1: Five capabilities, one management cycle

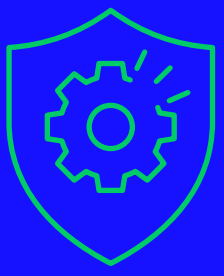
Source: MHP and zNT. Percentages meeting each criterion: zNT analysis of Civey raw data; n = 1,000 (see Methodology for definitions).

I The Gap Lies in Management

Our findings reveal a striking gap between companies' often-positive assessments of their own preparedness and the capabilities they have actually put in place.

3.1% of companies surveyed meet **all five criteria** for Defense Readiness

25% meet **none** of the criteria



The main shortfall is not a lack of awareness of potential threats. It is a lack of effective management of defense preparedness.

This is especially evident in digital and organizational resilience, including rehearsed fallback plans, clear responsibilities, and preparations for disruption. On average, companies lack 5.5 of the nine cyber resilience measures assessed, and 76 percent could sustain a complete IT outage for no more than three days. Physical capacity alone is therefore not enough. Without resilient control, communications, and recovery processes, those assets may be of limited use in an emergency. The risks are particularly acute in logistics and transportation, which are central to security of supply and military mobility.

What Needs to Happen Next

1. **UNDERSTAND**
   Identify the company's role and the capabilities critical to its contribution.

2. **PREPARE**
   Incorporate national and collective defense scenarios into strategy, risk management, and business continuity management.

3. **CONNECT**
   Make critical supply chains and dependencies visible, and establish clear points of contact and procedures linking government, civil protection authorities, and businesses.

4. **TEST**
   Exercise these capabilities regularly and jointly.

5. **IMPROVE**
   Learn from exercises and incidents, and continually update plans and performance metrics.

In other words, Defense Readiness requires measurable objectives, active oversight, and processes that have been tested under conditions of stress.

Companies rightly expect government to clarify what will be required of them in an emergency and to provide coordination and networks that support collaboration. In return, they are ready to cooperate. For example, 83 percent would be willing to report available capacity through a nationwide platform that shares information on readiness and operational capabilities.

Still, companies must develop much of their Defense Readiness themselves. The five core capabilities belong on the senior management agenda. For many businesses, executive management has also had explicit legal responsibilities since Germany's NIS2 Implementation Act took effect.Leadership teams need to close these gaps in the coming months and give this challenge sustained attention.

Contents

1. Germany's Mid-Market Companies Are Ready to Take Responsibility 8

Companies Often Lack Clarity About Their Role 09

The Size Gap: Smaller Companies Lag Behind 10

2. Defense Readiness Starts With Management 11

A Positive Self-Assessment Can Mask Operational Gaps 12

Cyber Resilience Is the Most Visible Weakness 15

Sustaining Operations and Recovering Systems Are Different Capabilities 16

3. From Willingness to Defense Readiness 18

Understand: Define the Company's Role and Capabilities 18

Prepare: Integrate Defense Scenarios Into Risk Management and Business Continuity Management 19

Connect: Make Supply Chains and Capacity Visible 20

Test: Exercise Coordination and Interfaces 21

Improve: Measure Readiness and Make Adjustments 22

Government and Industry Need a Shared Framework for Action 22

4. Conclusion: Making Defense Readiness Operational 24

Methodology and Context 25

1. Germany's Mid-Market Companies Are Ready to Take Responsibility

Companies no longer view changes in the security environment as solely a matter for government. Four out of five decision-makers say crisis resilience and defense preparedness have become more important to their industry over the past three years.

This recognition is an important foundation for whole-of-society resilience. It raises awareness, supports investment, and increases the willingness to contribute existing capacity to collective crisis preparedness.

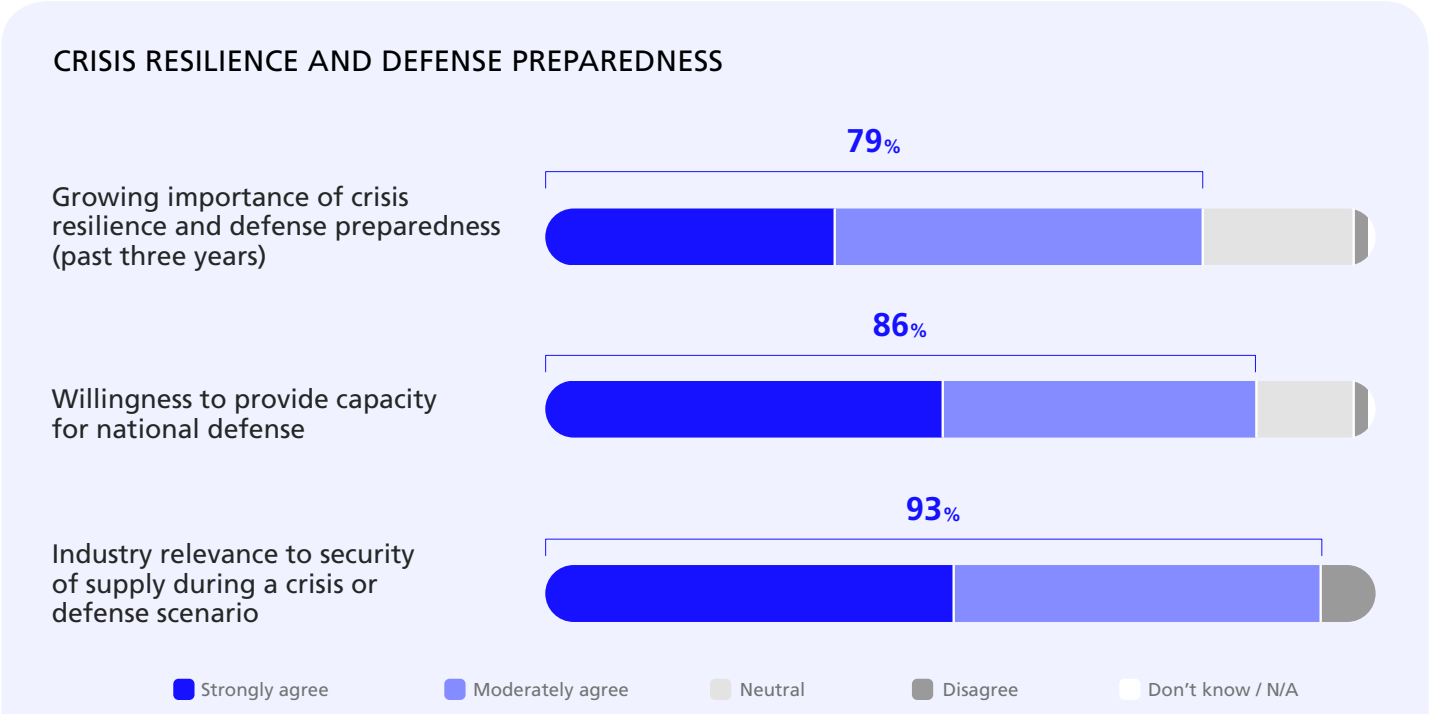


Figure 2: Importance, willingness, and relevance: broad support across the board

Source: Civey/MHP, Study Ready to Defend?, questions 1, 2, and 5; n = 1,000.
Figures show the combined share of strong and moderate agreement.

This willingness extends across industries. Overall, 86 percent would be willing to make capacity available, and 93 percent consider their industry relevant to maintaining supplies in Germany during a crisis or defense scenario.

The economic and societal willingness to engage is therefore present. The next challenge is to turn that willingness into specific, deliverable commitments.

Companies Often Lack Clarity About Their Role

An organization can make a reliable contribution only if it understands and has assessed its potential role. Yet this is far from universal: just 41.7 percent of companies have identified and assessed their role in a defense scenario. The gap between industries spans 36.7 percentage points. Financial services leads at 63.6 percent, while OEM suppliers rank last at 26.9 percent.

INDUSTRY COMPARISON

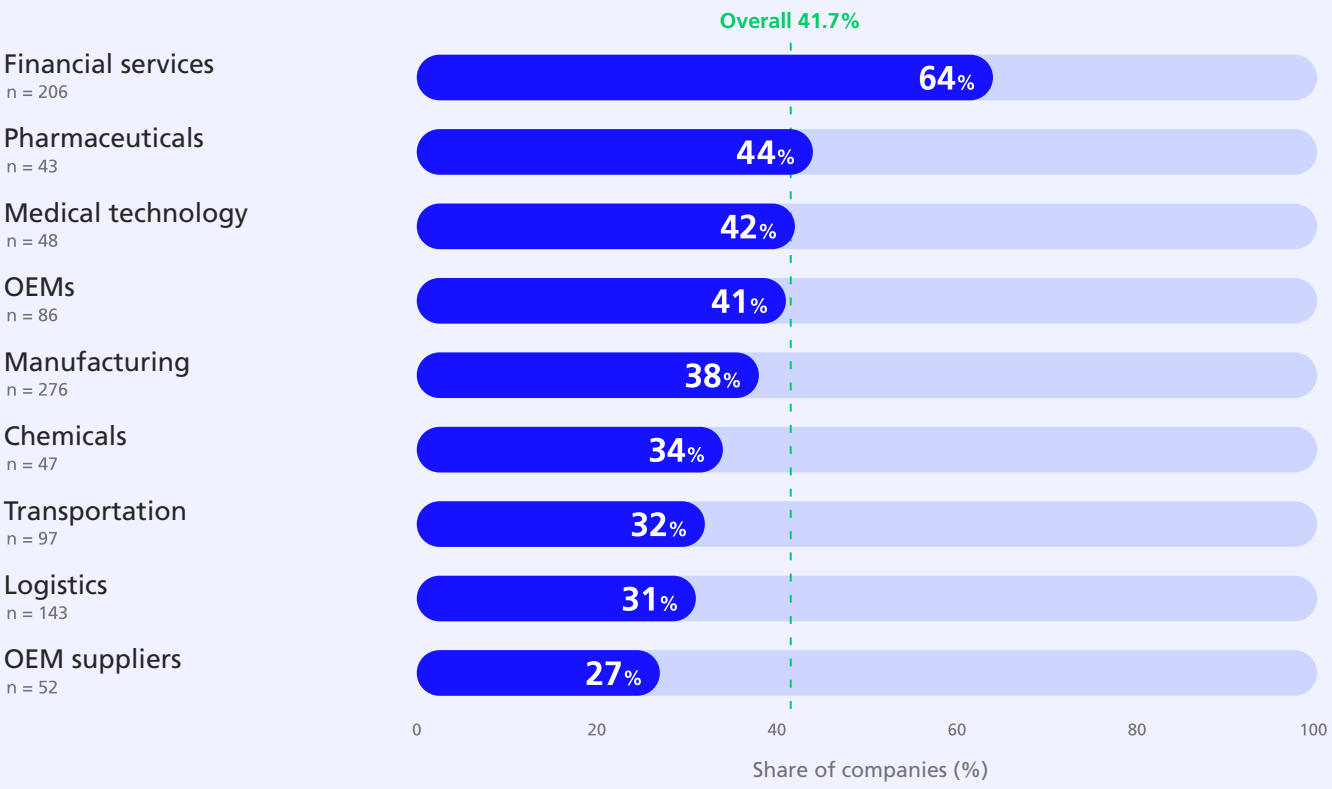


Figure 3: Assessment of the company's role, by industry

Source: zNT analysis of Civey raw data (question 16); n = 998
(excluding respondents unsure of their industry). Share answering "role identified and assessed."

These differences are statistically significant, although the association with industry is only moderate.[1] This suggests that industry alone does not explain the variation. Specific capabilities, dependencies, customer relationships, and connections with government are also relevant and differ among companies. Regulation may play a role as well. The EU's Digital Operational Resilience Act (DORA) has imposed comprehensive digital operational resilience requirements on financial institutions since January 2025. Financial services also leads in cyber resilience (see Chapter 2).

The Size Gap: Smaller Companies Lag Behind

Company size also matters. Among businesses with fewer than 250 employees, just 28 percent have identified and assessed their role, compared with 54 percent of those employing 1,000 to 5,000 people. Smaller companies are less likely to rate their own preparedness favorably (65 percent versus 80 percent). They are also much more critical of public-private cooperation on crisis preparedness: only 48 percent rate it positively, compared with 67 percent among companies with 1,000 to 5,000 employees.[2]

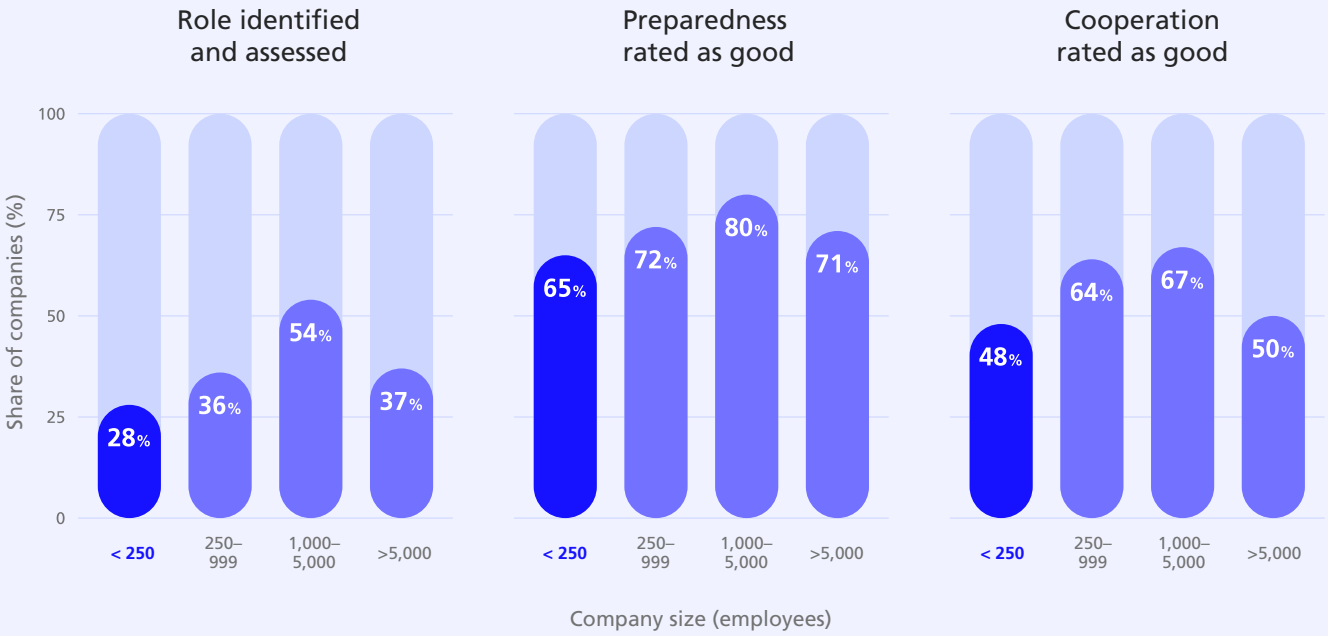


Figure 4: The size gap in role assessment, self-assessed preparedness, and views of cooperation

Source: zNT analysis of Civey raw data (questions 13, 15, and 16); n = 1,000. "Good" includes "very good" and "fairly good."

Notably, the largest companies, those with more than 5,000 employees, perform less well. Only 37 percent have assessed their role, and 50 percent rate public-private cooperation positively. Readiness, then, does not increase steadily with company size. Businesses with 1,000 to 5,000 employees score highest, while smaller firms lag behind. These are precisely the companies that may feel too small to establish dedicated structures but are too interconnected to wait out a crisis.

2. Defense Readiness Starts With Management

Based on our project experience and analysis of the survey data, we have identified five capabilities that form the foundations of Defense Readiness:

1. identifying and assessing the company's role
2. incorporating national and collective defense scenarios into risk management
3. understanding critical supply chains and dependencies
4. maintaining effective business continuity management
5. establishing organizational and technical cyber resilience, including recovery capabilities

These capabilities need to work together. A company may have employees, equipment, and logistics capacity yet still be unable to operate on short notice if its energy supply, IT, suppliers, or access to key contacts is disrupted. Readiness therefore describes the ability of the organization as a whole to withstand crises and shocks.

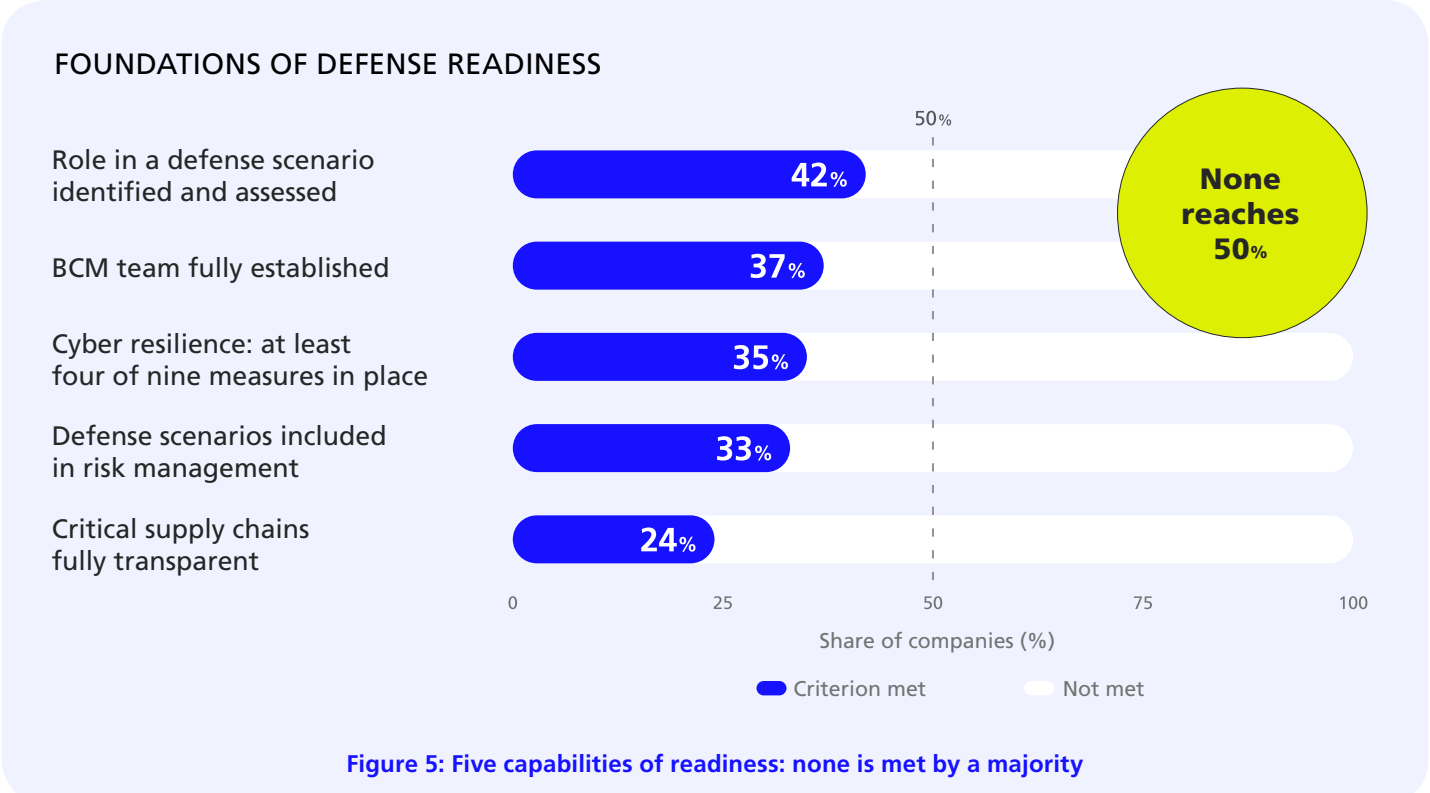


Figure 5: Five capabilities of readiness: none is met by a majority

Source: zNT analysis of Civey raw data (questions 6, 7, 8, 9, and 16); n = 1,000.
Results are based on different questions and are only partly comparable; see Methodology for index construction.

Currently, only 3.1 percent of the companies surveyed meet all five criteria. Another 25.1 percent meet none, 23.3 percent meet one, and 23.3 percent meet two.

In total, 48.4 percent meet no more than one criterion.

Only 3.1% meet all five criteria

DEFENSE READINESS CRITERIA MET

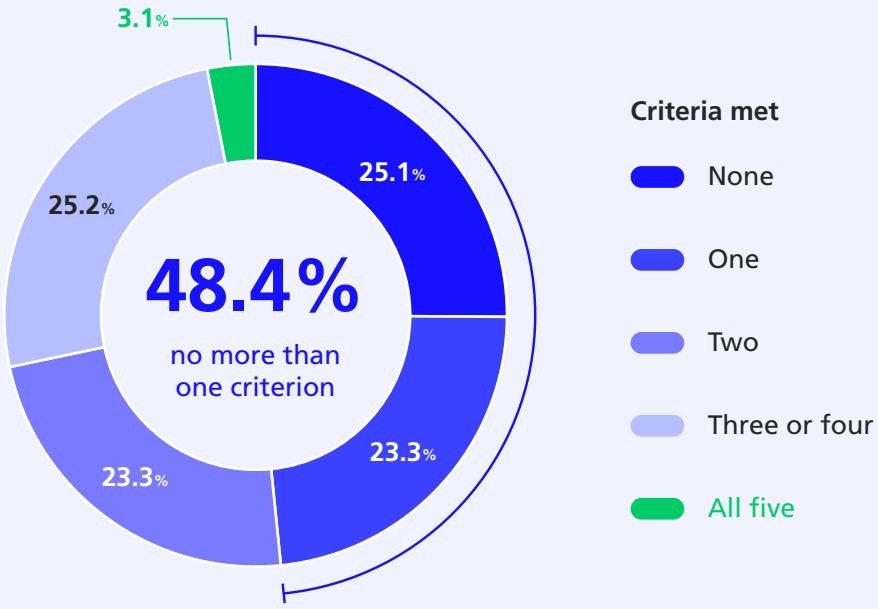


Figure 6: Defense Readiness at a glance: number of criteria met

Source: zNT analysis of Civey raw data; n = 1,000. Exploratory index ranging from zero to five criteria met.

This distribution explains why a single positive indicator, such as ample production capacity or a high willingness to contribute, cannot demonstrate genuine readiness.

These findings should be understood as exploratory self-reported data, not as the outcome of an independent audit. That distinction also makes them useful: confidence and operational preparedness do not necessarily develop at the same pace. A company can feel well prepared even when the systems and processes needed to support that confidence are not in place.

A Positive Self-Assessment Can Mask Operational Gaps

The relationship between perceived preparedness and the number of criteria met is clear, but hardly reassuring. Even among companies meeting no more than one criterion, 55.2 percent describe themselves as very or fairly well prepared. Of those meeting none, 46.2 percent still rate their preparedness positively. These findings suggest a pattern of overconfidence among companies that lack the underlying operational capabilities.

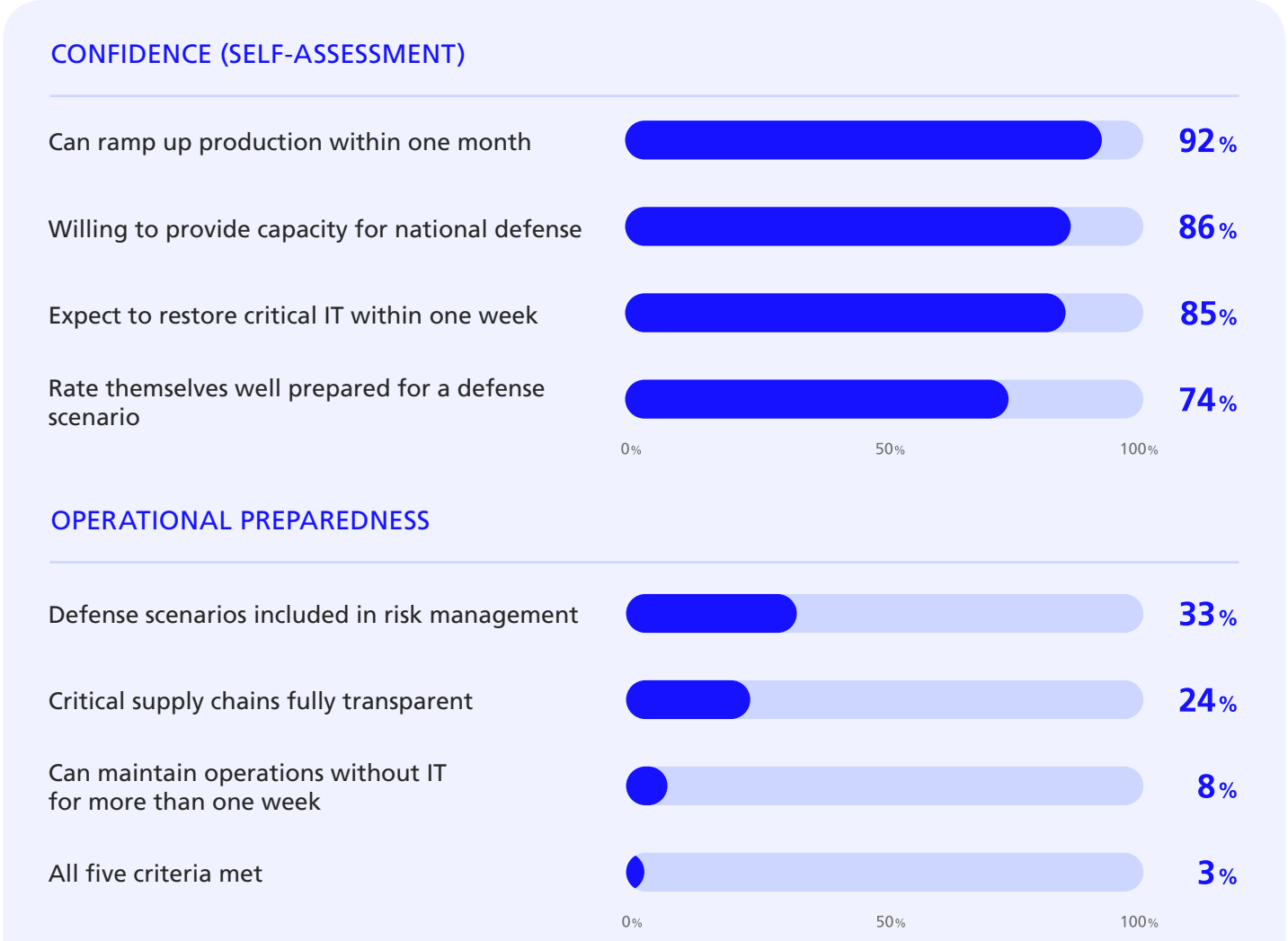


Figure 7: Confidence versus operational preparedness

Source: zNT analysis of Civey raw data (questions 3, 5–11, 15, and 16); n = 1,000.

For management teams, the implication is familiar from other areas of business: readiness must be measured and validated through scenarios and testing. Self-assessments are a useful starting point, but they cannot replace emergency drills, recovery tests, supply chain assessments, or established contacts in government.

Regulatory momentum: NIS2 makes resilience an executive responsibility

Germany's NIS2 Implementation and Cybersecurity Strengthening Act has been in force since December 6, 2025. Whether an organization is covered depends on the specific category of entity listed in Annexes 1 and 2 of the German Federal Office for Information Security Act (BSIG) and, generally, on its employee count, annual revenue, and balance sheet total. For many categories, the threshold is at least 50 employees, or annual revenue exceeding €10 million together with a balance sheet total exceeding €10 million. Different rules apply to certain categories. Companies in transportation and logistics, chemicals, pharmaceuticals, medical technology, and vehicle manufacturing may therefore fall within the scope, although not all businesses in those sectors are automatically covered. The BSI estimates that roughly 29,500 entities are affected; nearly 18,000 have registered as of the end of June 2026.

Obligations: Where the BSIG applies, section 30 requires risk management measures closely related to capabilities assessed in this study. These include business continuity management with backup and recovery procedures, incident management, supply chain security, and multi-factor authentication. For financial institutions covered by DORA, its cybersecurity risk management and major incident reporting requirements take precedence to the extent they are at least equivalent.

Executive accountability: For essential and important entities, section 38 of the BSIG requires executive management to implement and oversee the measures set out in section 30. Executives must participate in regular training and may be liable to their companies for damages caused by culpable breaches of duty. They cannot delegate this responsibility entirely to a CIO or CISO. For financial institutions subject to DORA, the remaining obligations under the BSIG must be assessed case by case.

For some of the surveyed companies, the gaps identified here therefore represent regulatory as well as strategic risks. Regulation can also help drive progress. Companies implementing NIS2 or DORA can incorporate national and allied defense scenarios into existing oversight, reporting, and exercise procedures. Germany's 2026 Critical Infrastructure Framework Act also requires operators of critical facilities to adopt physical resilience measures.

STATUTORY CYBERSECURITY OBLIGATIONS

Around

29,500

entities in Germany fall under NIS2.

Binding cybersecurity requirements.

Cyber Resilience Is the Most Visible Weakness

Not one of the measures assessed is in place at a majority of companies. Multi-factor authentication and around-the-clock monitoring each reach 46 percent, while just 27 percent report having an incident response team. On average, companies have implemented 3.5 of the nine measures. The combination of dependence on digital systems and inadequate recovery arrangements is particularly concerning.

CYBER RESILIENCE: MEASURES IN PLACE

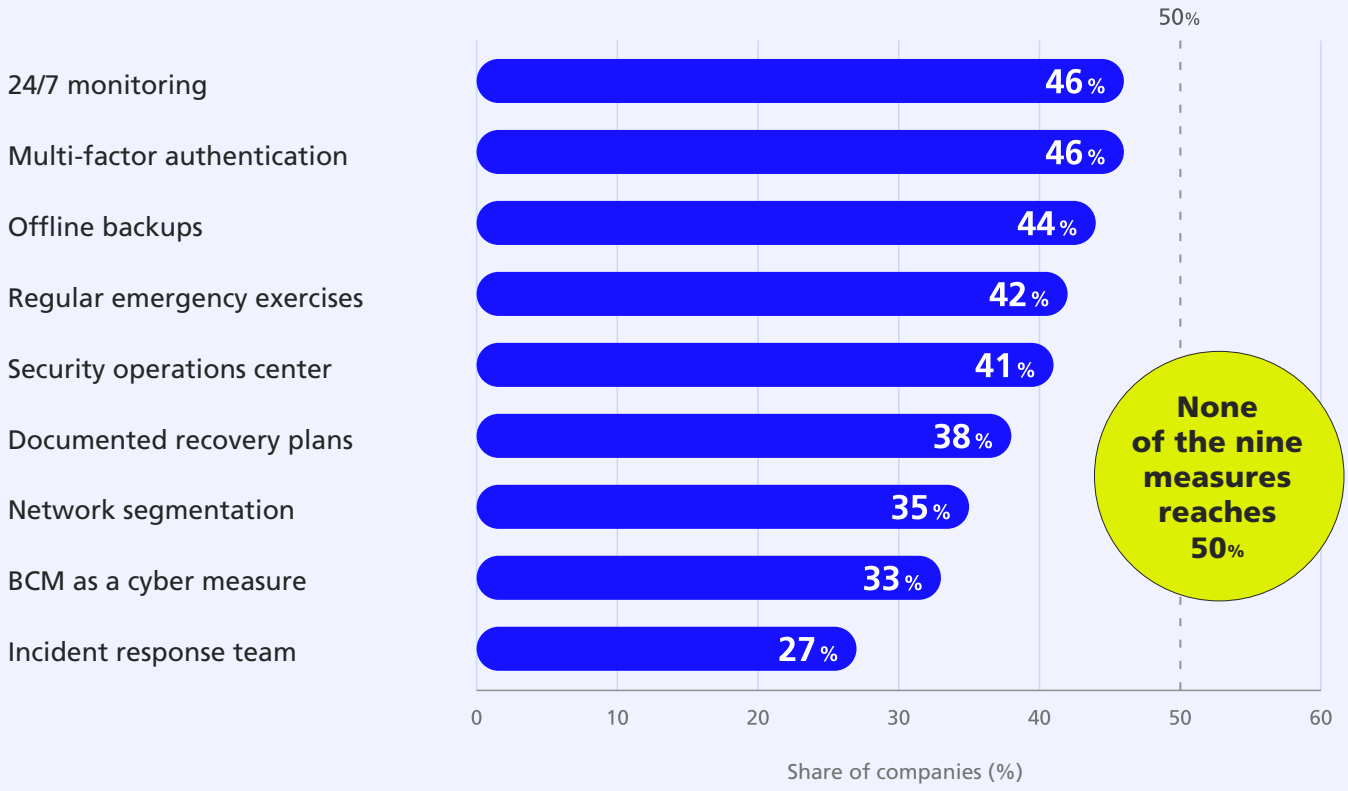
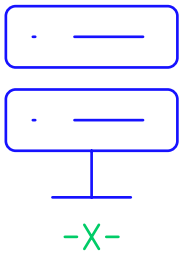


Figure 8: Cyber resilience: no single measure reaches a majority

Source: Civey/MHP, Defense survey, question 9 (multiple responses); n = 1,000.

The gap is most pronounced in logistics and transportation. Companies in these sectors have implemented an average of just 2.7 and 2.8 of the nine measures, respectively, compared with 4.2 in financial services. Yet logistics and transportation are essential to security of supply and military mobility. Having trucks or warehouse space available is of limited value if dispatch, communications, telematics, or billing systems fail after a cyberattack.

Sustaining Operations and Recovering Systems Are Different Capabilities



A total of 76 percent of companies could maintain operations for no more than three days if critical IT systems failed completely. For 46 percent, the limit would be 24 hours or less. This is a measure of operational endurance, which is not the same as recovery capability.

OPERATIONS DURING AN IT OUTAGE

How long could operations continue after a complete IT outage?

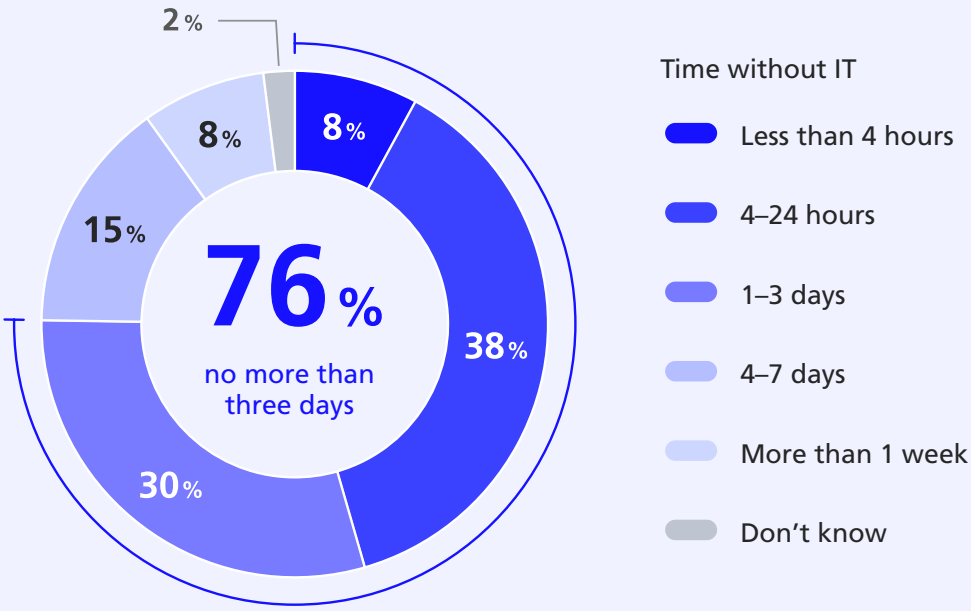


Figure 9: How long operations could continue after a complete IT outage

Source: Civey/MHP, Defense survey, question 10; n = 1,000.

Rapid production ramp-up, limited IT outage tolerance

Cross-tabulated results reveal another disconnect between confidence and capability. Among companies that say they could ramp up production within one week in a defense scenario (69 percent of all companies surveyed), about half (51 percent) could withstand a complete IT outage for no more than 24 hours. Among those confident of ramping up within 24 hours, the share rises to 61 percent, well above the overall average of 46 percent. The most confident companies are therefore particularly dependent on functioning IT systems.

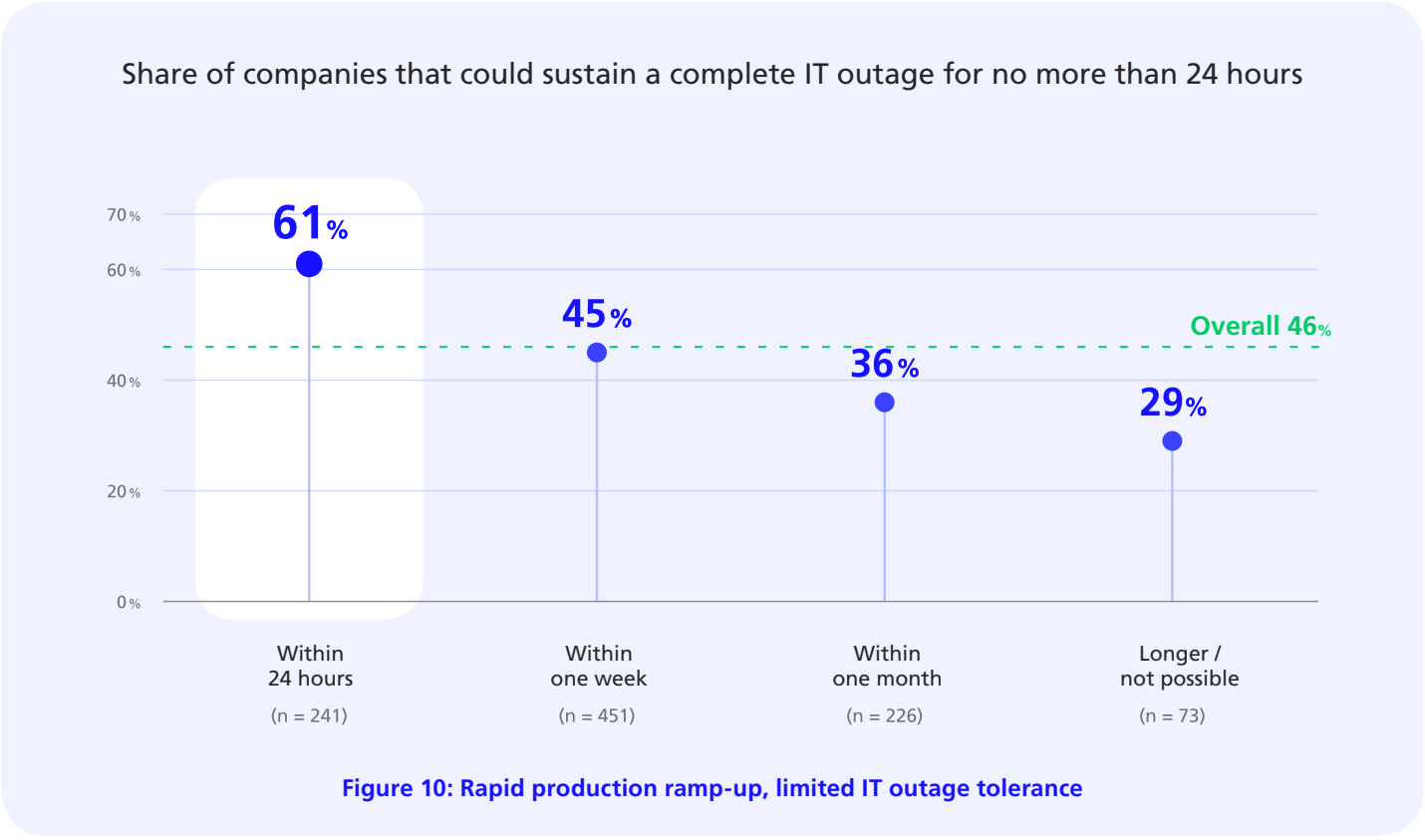


Figure 10: Rapid production ramp-up, limited IT outage tolerance

Source: zNT analysis of Civey raw data (questions 3 and 10); n = 991 (excluding "don't know" responses to question 3).

The ability to sustain operations must be distinguished from the ability to restore systems. In zNT's cross-tabulation, 92 percent of companies that could tolerate an IT outage of up to three days also believed they could restore business-critical IT within one week of a large-scale cyberattack. Among companies with an outage tolerance of at least four days, the share was only 68 percent.[3]

A longer outage tolerance does not automatically indicate greater readiness. It may also reflect that less priority has been given to developing recovery procedures. The data do not establish a causal relationship. Differences in technical architecture, decentralized systems, manual fallback procedures, or deliberately built-in buffers may help explain the findings. The conclusion for management is that operational endurance and recovery capabilities need to be planned and tested separately.

3. From Willingness to Defense Readiness

The findings show that companies are highly willing to contribute. But Defense Readiness depends on what they can actually deliver in an emergency: in what quantities, with how much lead time, and for how long. Companies therefore need to understand their roles and capabilities, make critical dependencies visible, prepare for different scenarios, test recovery and supply arrangements, and define how they will coordinate with government agencies. The priorities below are organized along the management cycle.

I Understand: Define the Company's Role and Capabilities

The starting point is an assessment of the company's potential role. That should lead to a clear capability profile: What can the company provide, in what quantity and quality, with what lead time, for how long, and subject to which dependencies? Companies cite staff shortages (46 percent), material shortages (38 percent), and lengthy approval processes (34 percent) as the biggest barriers to providing additional capacity.

Key steps:

- describe and document critical services and capabilities
- quantify available capacity and dependencies on personnel, energy, and IT
- identify contacts and establish escalation paths
- review legal and contractual requirements

Government can provide guidance, scenarios, priorities, and points of contact. Companies, however, must understand their own capabilities and update that assessment regularly.

Prepare: Integrate Defense Scenarios Into Risk Management and Business Continuity Management

Only 33 percent of companies have already included a national and collective defense scenario in their risk management. For nearly two-thirds (65 percent), such planning is at best at the planning stage. Only 37 percent have fully established a business continuity management (BCM) team to protect critical operations. This leaves many companies without a clear link between general crisis preparedness and specific defense scenarios. Where risk, crisis, and business continuity processes already exist, they should be adapted to address those scenarios. For critical services, companies should define minimum operating levels, recovery time objectives, alternative resources, and clear responsibilities.

Four steps are needed:

1. incorporate defense scenarios into risk management
2. prioritize business processes and define minimum operating levels
3. document recovery plans for IT, energy, staffing, and logistics
4. conduct regular exercises based on realistic assumptions

The question is not simply whether a plan exists, but whether it works under pressure. Exercises should therefore simulate incomplete information, disruptions at service providers, and conflicting situation reports.

Connect: Make Supply Chains and Capacity Visible

For three-quarters of companies, critical supply chains are not fully transparent to external stakeholders across multiple supplier tiers. Only 24 percent describe them as fully transparent. Supply chains that cannot be made visible are also difficult to incorporate into a common operating picture. Respondents living in large cities are somewhat more likely than those in rural areas to report at least mostly transparent supply chains (74 percent versus 63 percent). Because the survey records respondents' place of residence rather than their companies' locations, this provides only limited evidence of regional differences.[4]

At the same time, 83 percent would be willing to participate in a nationwide platform for reporting available capacity. This offers a practical starting point: willingness can be translated into a current, structured view of operating conditions and capacity. To support decisions, data on critical capacity and dependencies must be available in a usable format. In addition to quantities, the information should include lead times, operating endurance, dependencies, alternatives, and current status.

Key steps:

- map critical supply chains and single points of failure
- assess alternative sources of supply and regional bottlenecks
- report available capacity, lead times, and how long operations can be sustained
- define data quality standards, update cycles, and access rights

A platform does not replace decision-making. It can, however, allow government and industry to work from the same operational picture during an emergency. That does not necessarily require a new centralized data repository. Existing systems and data sources can be connected through interoperable interfaces to provide a shared view of capacity, constraints, and alternatives. The value lies in using that information to set priorities, redirect resources, and respond to disruptions.

Test: Exercise Coordination and Interfaces

Companies say that the most useful forms of government support would be regular information sharing (43 percent), a clear legal framework (40 percent), financial incentives (39 percent), standardized procedures (38 percent), and designated points of contact (33 percent). Digital platforms are cited by 29 percent. These responses suggest a coordination problem: companies are willing to contribute, but the mechanisms for activating that contribution are not sufficiently standardized. Notably, joint exercises rank last at 26 percent, even though they are one of the clearest ways to test whether arrangements work in an emergency.

INFORMATION SHARING COMES FIRST

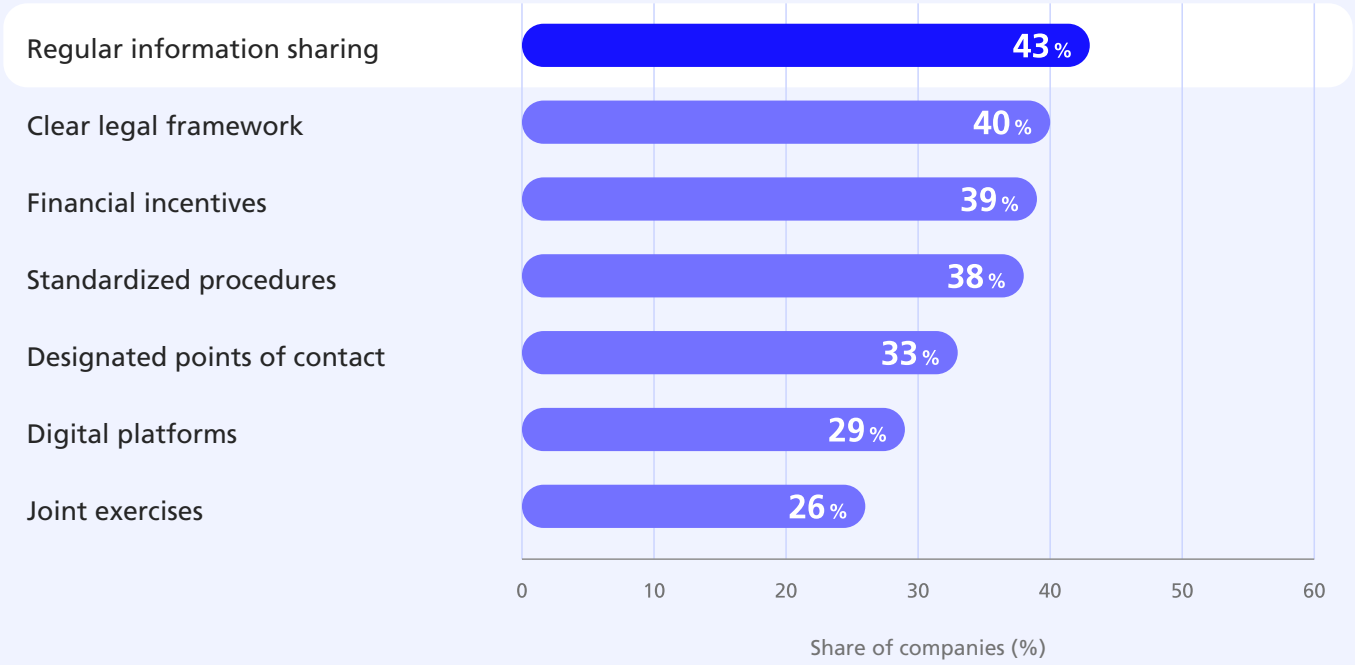


Figure 11: What would make it easier for companies to contribute during a crisis

Source: Civey/MHP, Defense survey, question 12 (government support measures, multiple responses); n = 1,000.

This requires:

- joint exercises involving government, companies, and critical service providers
- designated contacts, deputies, and escalation procedures
- clear rules for liability, compensation, prioritization, and information protection
- a review after every exercise, with binding follow-up actions

Effective cooperation is measured by whether agreed procedures still work under time pressure.

Improve: Measure Readiness and Make Adjustments

Defense Readiness requires regular review and adjustment. Every exercise, incident, and change in circumstances can expose weaknesses in plans, reported capacity, or interfaces. Companies should therefore establish a small set of meaningful metrics, such as the share of critical services with documented capability profiles, tested recovery times, or how current their capacity data is. Senior management should review these metrics regularly. Where NIS2 applies, they can be integrated into existing monitoring and reporting obligations.

Government and Industry Need a Shared Framework for Action

The findings point to a division of responsibilities. Companies are responsible for understanding their capabilities, strengthening internal resilience, and keeping their data current. Government must provide scenarios, priorities, contacts, a clear legal framework, and secure means of sharing information. Current perceptions of public-private crisis preparedness show how much work remains: only 62 percent of companies rate cooperation as good, while 17 percent rate it as poor. The assessment is less favorable in transportation (53 percent) and logistics (54 percent) than in financial services (78 percent), and among smaller companies (48 percent).

Who Is Responsible for What

Companies

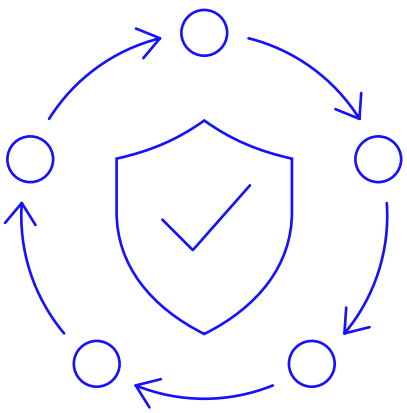
- understand their critical services and available capacity
- prepare for scenarios and recovery
- keep information and capability profiles current
- test their capabilities regularly

Government

- define scenarios, requirements, and priorities
- designate contacts and procedures for activating support
- establish the legal framework
- provide secure information-sharing channels
- coordinate activities and maintain a shared operating picture

Joint responsibilities

- record capacity and make dependencies visible
- build a common operating picture, activate capabilities, and manage bottlenecks
- run exercises, improve interfaces, and regularly test cooperation



The goal is a Defense Readiness management approach built around five recurring activities: understand, prepare, connect, test, and improve. Together, they turn an intention into a capability that can be demonstrated.

4. Conclusion: Making Defense Readiness Operational

German businesses are highly willing to take responsibility in a crisis or defense scenario. Yet the study identifies a clear gap between that willingness, companies' own assessments, and their operational preparedness.

Closing this gap will take more than a single investment. It requires defining roles, managing risk, strengthening supply chains, establishing business continuity management, improving cyber resilience, and working more effectively with government agencies. Especially concerning are the above-average cyber resilience gaps in logistics and transportation, sectors essential to security of supply and military mobility, as well as the limited clarity smaller companies have about their potential roles.

Defense Readiness is not a one-time achievement. It is an ongoing management process. Companies need to understand their capabilities, practice scenarios, maintain current data, and test recovery procedures. Government agencies need to provide clear frameworks, designated contacts, and secure channels for exchanging information. Only by working together can government and industry put economic capacity to use when it is needed most.

Defense Readiness means knowing a company's role, available capabilities, dependencies, and ability to sustain operations, and reassessing them regularly. Ultimately, **the question is simple: What can a company actually deliver in an emergency, in what quantities, with what lead time, for how long, and under what** conditions? Willingness becomes credible defense capability only when that capacity is known, can be planned for, and can be activated when needed.

Methodology and Context

Data Basis

The study is based on a survey of 1,000 private-sector decision-makers in Germany conducted by Civey between July 31 and August 17, 2026. Respondents held positions at team-lead level or above across a range of industries at companies with annual revenue of at least €50 million and no more than €5 billion. The sample covers manufacturing (28 percent), financial services (21 percent), logistics (14 percent), transportation (10 percent), original equipment manufacturers (OEMs, 9 percent), OEM suppliers (5 percent), and medical technology, chemicals, and pharmaceuticals (roughly 4 to 5 percent each). The reported statistical margin of error for the overall results is 3.1 percentage points.

Analysis

The analysis draws on Civey's results and additional work by zNT using the raw survey data, including cross-tabulations, significance tests, and index construction. All values in this study were calculated from the raw data and rounded. They may therefore differ by one percentage point from Civey reports that sum rounded individual values. Totals may not sum to 100 percent.

The Readiness Index is based on five criteria. Each is counted as met when the applicable condition is satisfied; the total produces an exploratory score from zero to five. The index is intended to organize the results and is not a substitute for an independent audit.

Criterion	Question	Condition for meeting the criterion	Share
Role assessment	16	"Role identified and assessed"	41.7%
Risk management	6	National or allied defense scenarios "already considered"	33.0%
Supply chain transparency	7	Critical supply chains "fully transparent" to external stakeholders	23.7%
Business continuity management	8	BCM team "fully established"	36.8%
Cyber resilience	9	At least four of nine measures in place	35.2%

Source: zNT analysis of Civey raw data; n = 1,000.

Limitations

The findings are based on self-reported information. They capture perceptions, the stated status of measures, and exploratory associations, not independently verified technical or organizational effectiveness at individual companies. Industry and size comparisons should be interpreted with caution where subgroup samples are small; very small groups are not reported separately. Regional analyses use respondents' home locations rather than company locations. Correlations should not be interpreted as evidence of causation.

Sources

Civey/MHP: Defense survey, July 31–August 17, 2026; n = 1,000.

zNT, Center for Sustainable Transformation: independent analyses of Civey raw data.

German Federal Office for Information Security (BSI): NIS2 obligations; NIS2 in numbers (as of June 30, 2026), www.bsi.bund.de.

German NIS2 Implementation and Cybersecurity Strengthening Act (NIS2UmsuCG), effective December 6, 2025; sections 30 and 38 of the BSIG.

German Critical Infrastructure Framework Act (KRITISDachG), Federal Law Gazette 2026 I No. 66.

Regulation (EU) 2022/2554 on digital operational resilience in the financial sector (DORA), applicable since January 17, 2025.

Notes

[1] The association between industry and complete role assessment is statistically significant ($\chi^2(8) = 57.7$; $p < 0.001$), although the effect size is limited (Cramér's V = 0.24).

[2] Group sizes: fewer than 250 employees: n = 141; 250–999: n = 384; 1,000–5,000: n = 391; more than 5,000: n = 84. Differences are statistically significant (role assessment: $\chi^2(3) = 41.2$; $p < 0.001$; self-assessed preparedness: $\chi^2(3) = 13.2$; $p = 0.004$; cooperation: $\chi^2(3) = 21.1$; $p < 0.001$). The group with fewer than 50 employees is not reported separately because of its small sample size (n = 28).

[3] Based on companies that provided a valid estimate of the time needed to restore systems (question 11).

[4] Share reporting "fully" or "mostly transparent": large cities 74.1 percent (n = 421), small and midsize cities 65.8 percent (n = 404), rural areas 63.4 percent (n = 175); $\chi^2(2) = 9.5$; $p = 0.008$; Cramér's V = 0.10.

Layout & Design: www.freiland-design.de

Contacts

MHP Management and IT Consulting GmbH

John Eisenhauer
Partner
Head of Public & Defense
john.eisenhauer@mhp.com

zNT, Center for Sustainable Transformation at Quadriga University Berlin

Prof. Dr. Torsten Oltmanns
Managing Partner
torsten.oltmanns@znt-berlin.com

MHP Management and IT Consulting GmbH
Film- und Medienzentrum
Königsallee 53
D-71638 Ludwigsburg
Email info@mhp.com