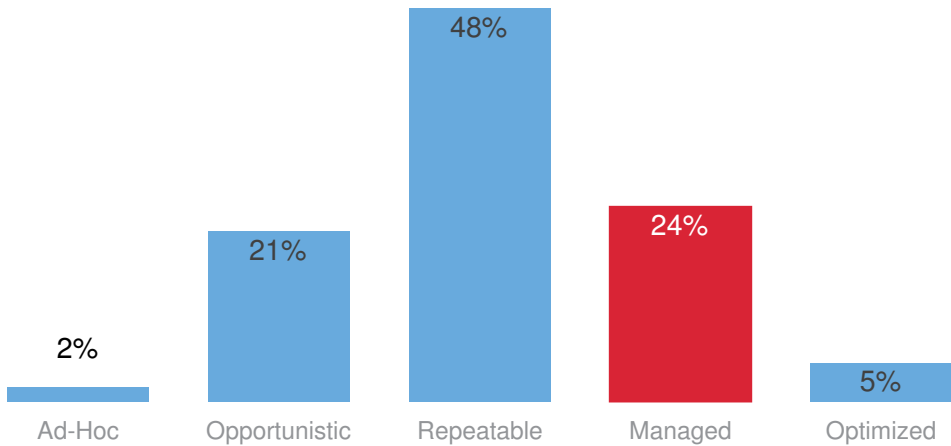# CUSTOM REPORT SUMMARY AND OVERALL PERFORMANCE RANKING
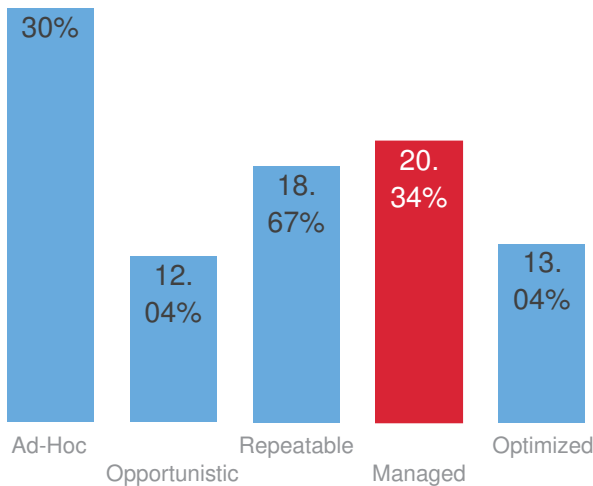
## How you compare overall
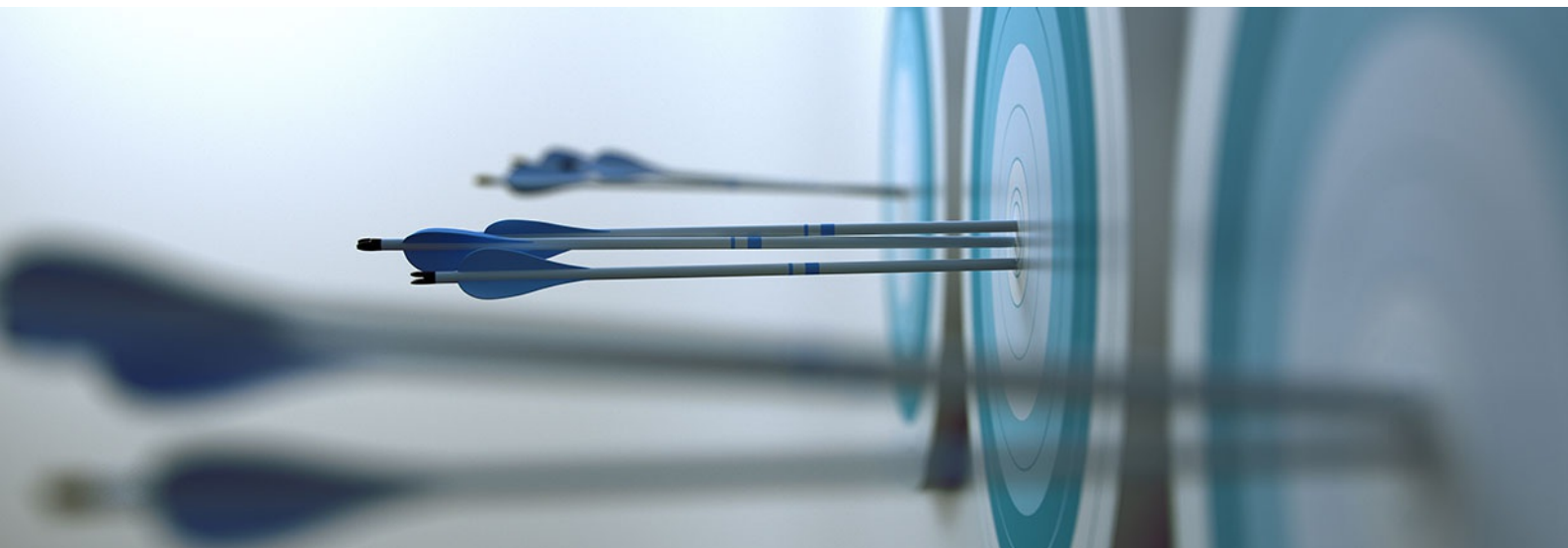


| Ad-Hoc | Opportunistic | Repeatable | Managed | Optimized |
|--------|---------------|------------|---------|-----------|
| 2% | 21% | 48% | 24% | 5% |

## Your comparison to others in your country



| Ad-Hoc | Opportunistic | Repeatable | Managed | Optimized |
|--------|---------------|------------|---------|-----------|
| 0% | 21.3% | 25.31% | 12.71% | 4.35% |
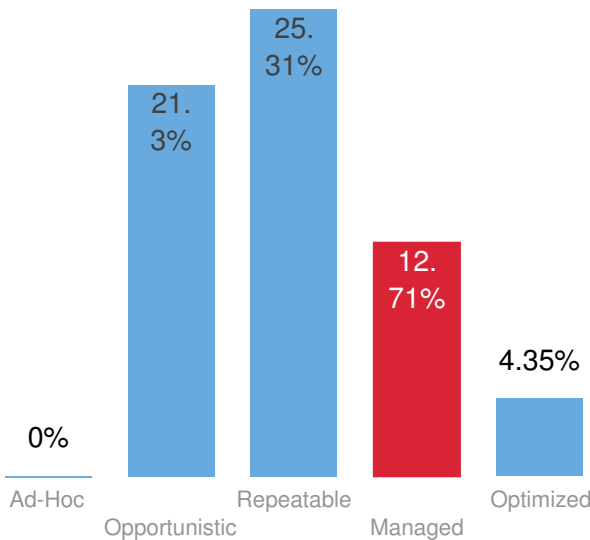
## Your comparison to companies of similar size



| Ad-Hoc | Opportunistic | Repeatable | Managed | Optimized |
|--------|---------------|------------|---------|-----------|
| 30% | 12.04% | 18.67% | 20.34% | 13.04% |

FireEye | DXC.technology

# PERFORMANCE RANKING BY CATEGORY

## Cyber Risk Management and the Business

**INLINE**

Ranking: **MANAGED**

Impressive showing! You are in-line in this core area of Cyber Risk management,, but should still look to emerging ways to improve your ability to secure your IT domain.

## Cyber Risk Management Operations and Defence

**AHEAD**

Ranking: **MANAGED**

Top of the class! You are performing ahead of your peers in this area of Cyber Risk management but can always find ways to improve over time as new approaches emerge.

## Cyber Risk Management Breach Detection and Remediation

**AHEAD**

Ranking: **REPEATABLE**

Top job! You are ahead of your peers when it comes to managing Cyber Risk in conjunction with the business. You are performing very well in this area of Cyber Risk management but should not become complacent and continually reassess what you do.

FireEye | DXC.technology

# CYBER RISK MANAGEMENT AND THE BUSINESS PERFORMANCE RANKING BY QUESTION

We're now going to look at how you performed in three key areas of Cyber Risk Readiness. In each case, we'll look at how you compared to others in the same readiness ranking of **Managed** as yourself. To do this, we look at whether you are behind, in-line or ahead of your peers.

If you are in-line, you are broadly comparable to most companies at your level of readiness. If you are ahead, you are doing well in this area and should be looking at other areas to improve to get a balanced approach. If you are behind, you need to focus attention and investment in this area to bring your Cyber Risk Readiness in to line.

If you achieve a rating of in-line or ahead in all sections, you are ready to be moving up a readiness level in short order."

**Q1:** How does senior business management tend to view the role of IT? Please select one
A: **A driver of competitive advantage or differentiation**
When compared with the next level, **Optimized** you would be positioned as **Inline**

**Q2:** When it comes to business requests for new or enhanced applications or services, which statement best reflects your IT department's capabilities? Please select one
A: **We struggle to deal with most requests.**
When compared with the next level, **Optimized** you would be positioned as **Behind**

**Q3:** Which statement best describes your attitude to risk at a business level? Please select one
A: **We tend to avoid risks, but will take some risks where there is a very good justification.**
When compared with the next level, **Optimized** you would be positioned as **Behind**

**Q4:** Which of the following do you already have in place to protect your business in the event of an incident?
A:

| A formal risk assessment **Currently have** | Proactive detection (solutions that are able to identify unknown threats through techniques such as behavioural analytics and machine learning, as opposed to being reliant on blocking known threats through the use of signatures) **Don't have, but planned** | Response plan **No, and no plans** |
| Internal communications plan **No, and no plans** | External communications and public relations plan **No, and no plans** | Breach notification plan **No, and no plans** |
| Breach remediation plan **No, and no plans** | Cyber risk insurance **No, and no plans** | |

When compared with the next level, **stage5** you would be positioned as **Behind**

**Q5:** Which statement best describes how cyber risk management is handled in your company? Please select one
A: **It is typically delegated to IT or senior management**
When compared with the next level, **Optimized** you would be positioned as **Behind**

Q6: **Of the following, who are part of your cyber risk assessment structure?**
A:

| CEO | CFO | COO |
| No | Yes | Yes |

Non-executive board-level risk/compliance/security focused member
Yes

Executive board-level risk/compliance/security focused member
Yes

Dedicated risk/compliance/security role (non-board)
Yes

When compared with the next level, **stage5** you would be positioned as **Behind**

Q7: **How early is IT security usually brought into business projects and initiatives? Please select one**
A: **During planning**

When compared with the next level, **Optimized** you would be positioned as **Behind**

Q8: **How would you describe the level of IT security investment in your organization? Please select one**
A: **Good for core operations, but tight for new initiatives**

When compared with the next level, **Optimized** you would be positioned as **Behind**

# CYBER RISK MANAGEMENT OPERATIONS AND DEFENCE PERFORMANCE RANKING BY QUESTION

We're now going to look at how you performed in three key areas of Cyber Risk Readiness. In each case, we'll look at how you compared to others in the same readiness ranking of **Managed** as yourself. To do this, we look at whether you are behind, in-line or ahead of your peers.

If you are in-line, you are broadly comparable to most companies at your level of readiness. If you are ahead, you are doing well in this area and should be looking at other areas to improve to get a balanced approach. If you are behind, you need to focus attention and investment in this area to bring your Cyber Risk Readiness in to line.

If you achieve a rating of in-line or ahead in all sections, you are ready to be moving up a readiness level in short order."

**Q9:** To what level do you have the following in place for managing your IT physical security?
A:

| | | |
|---|---|---|
| Security staff screening 2 | Prebooked appointments 3 | Identity verification 4 |
| Man-traps to enter/exit 5 | Biometric authentication 1 | CCTV monitoring 1 |
| Man-shadowing (staff and visitors must work in pairs or be accompanied) 1 | Change authorization, approval, and logging 1 | |

When compared with the next level, **stage5** you would be positioned as **Behind**

Q10: **Which of the following best describes your adoption and implementation of IT security best practice? Please select one**
A: **We do this on a formal basis (using standards) using our general skills.**
When compared with the next level, **Optimized** you would be positioned as **Behind**

Q11: **How prepared are you for the following aspects of your assessment and implementation of GDPR (General Data Protection Regulation) compliance?**
A:

| | | |
|---|---|---|
| Knowledge of obligations 1 | Assessment of capabilities and gaps 3 | Implementation planning 5 |
| Implementation execution 4 | Continuous improvement/best practice beyond the GDPR itself (beyond the regulations) 4 | Understanding mitigation of penalties based on early detection/remediation 1 |

When compared with the next level, **stage5** you would be positioned as **Behind**

Q12: **Do you tend to invest tactically (point products/as needed) or strategically (part of a plan) in IT security products or solutions? Please select one**
A: **We have a balance of tactical versus strategic purchasing.**
When compared with the next level, **Optimized** you would be positioned as **Behind**

Q13: **How often do you report on IT security status to the business? Please select one**
A: **Annually**
When compared with the next level, **Optimized** you would be positioned as **Behind**

Q14: What is your primary means of managing your IT security infrastructure? Please select one

A: We use an end-to-end security management suite.

When compared with the next level, **Optimized** you would be positioned as **Inline**

Q15: To what level have you adopted automation in your IT security management? Please select one

A: Automation across the board

When compared with the next level, **Optimized** you would be positioned as **Inline**

Q16: When it comes to your use of automation, how do you intend to change your use of this? Please select one

A: Stay the same

When compared with the next level, **Optimized** you would be positioned as **Behind**

Q17: Do you make use of the following regarding IT security?

A:

NGFW (next-generation firewall)
No

IPS/IDS (intrusion detection/protection)
Yes

Vulnerability management
Yes

Micro segmentation (fine-grained separation and isolation of traffic between specified hosts or domains)
Yes

Unified security management (data and information interchange between devices and tools),
Yes

Third-party professional security service (pre-sales/design/implementation)
Yes

When compared with the next level, **stage5** you would be positioned as **Behind**

Q25: Which statement describes the extent of your use of managed security services providers? Please select one

A: We use them in a balanced way.

When compared with the next level, **Optimized** you would be positioned as **Behind**

# CYBER RISK MANAGEMENT BREACH DETECTION AND REMEDIATION PERFORMANCE RANKING BY QUESTION

We're now going to look at how you performed in three key areas of Cyber Risk Readiness. In each case, we'll look at how you compared to others in the same readiness ranking of **Managed** as yourself. To do this, we look at whether you are behind, in-line or ahead of your peers.

If you are in-line, you are broadly comparable to most companies at your level of readiness. If you are ahead, you are doing well in this area and should be looking at other areas to improve to get a balanced approach. If you are behind, you need to focus attention and investment in this area to bring your Cyber Risk Readiness in to line.

If you achieve a rating of in-line or ahead in all sections, you are ready to be moving up a readiness level in short order."

Q18: **Do you make use of the following regarding IT Security: Breach detection**
A:

Threat intelligence services
No

Real-time analytics
No

Advanced threat protection/sandboxing
No

AI/heuristics
No

Malware detection
No

When compared with the next level, **stage4** you would be positioned as **Behind**

Q19: **Do you make use of the following regarding IT Security: Breach response**
A:

Intelligence gathering solutions such as 'honeypots'
No

Forensic logging and analysis
No

Failover/system recovery
No

Tiger/go teams
No

External incident response partner
No

When compared with the next level, **stage4** you would be positioned as **Behind**

Q20: **Do you make use of the following regarding IT Security: Breach response**
A:

automated breach response (e.g. machine learning)
Yes

Policy updates
Yes

Disaster recovery policy
Yes

External disaster recovery providers
Yes

Compromise assessments
Yes

When compared with the next level, **stage4** you would be positioned as **Ahead**

Q21: **Have you done the following in regards to understanding your Cyber risk profile?**
A:

Assessed your risk of suffering a cyber breach
No

Understand potential scale of exposure
Yes

Done a data assessment of critical data
Yes

Understand posture of extended supply chain or partners
Yes

Developed a security breach response plan
Yes

When compared with the next level, **stage4** you would be positioned as **Inline**

FireEye | DXC.technology

Q23: **How often do you test your IT security defense capabilities through third-party verification? Please select one**
A: **Every quarter**

When compared with the next level, **Managed** you would be positioned as **Inline**

Q24: **How often do you test your cyber breach incident response plans? Please select one**
A: **Weekly**

When compared with the next level, **Managed** you would be positioned as **Ahead**