Governance & Management SCORECARD

Fill out by yours

Lean42

PREPARED FOR:

Mike Buma, Strategy Analyst and Product Owner
Info-Tech Research Group

IT SECURITY
DIAGNOSTIC PROGRAM
Powered by Info-Tech Research

INFO~TECH
RESEARCH GROUP

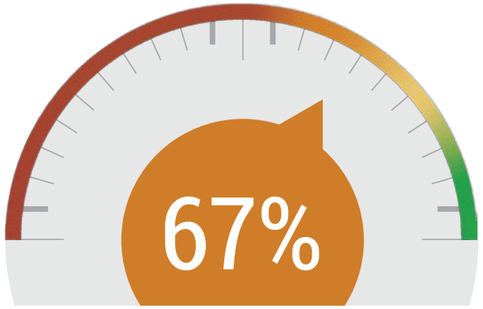
Security Governance and Management Maturity Scorecard

Info-Tech Research Group

Prepared for:
Mike Buma, Strategy Analyst and Product Owner

powered by INFO~TECH RESEARCH GROUP

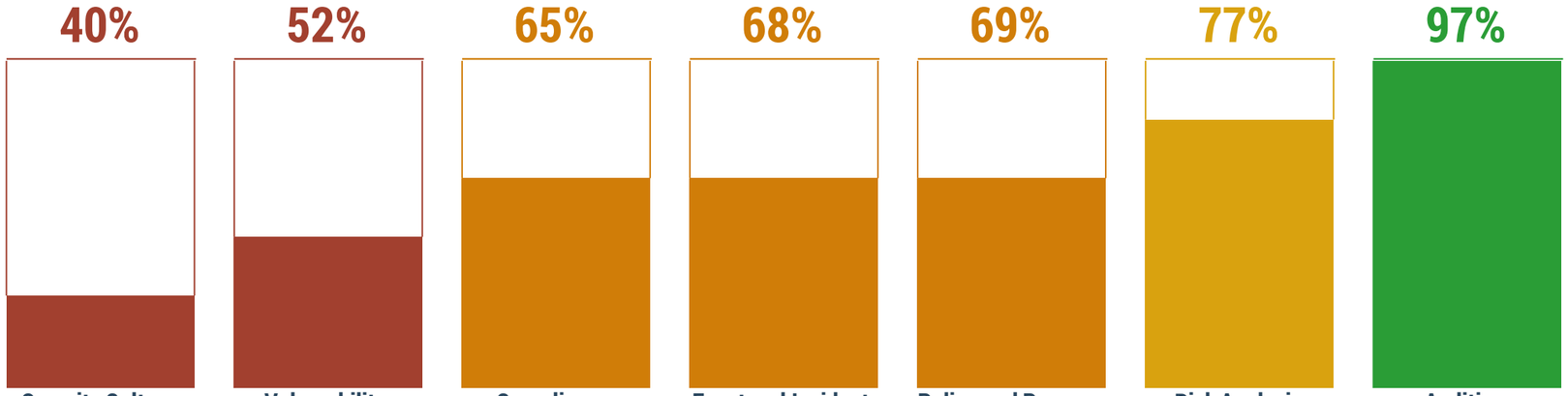
Overall Maturity Score



Measuring and communicating success in IT Security can be difficult. This score is a summary indicator of where you're at in relation to industry standard best practices.

Scores by Governance and Management Area

Use this information to identify and prioritize opportunities for improvement.

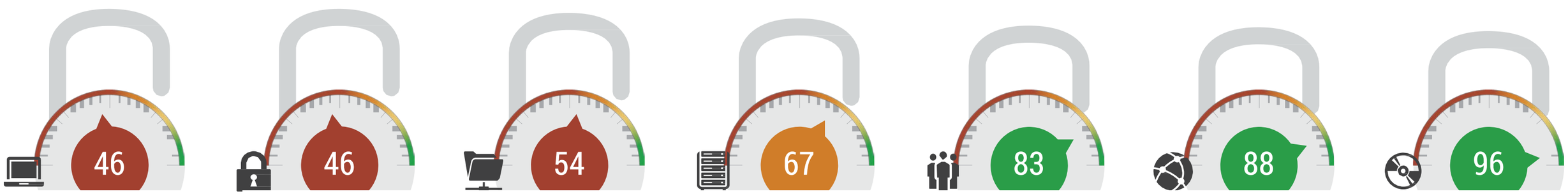


Evaluate overall security maturity as well as across 7 governance areas. Determine which areas require the most improvement and use this report to investigate improvement opportunities..

ecurity Culture, Vulnerability Management, and Compliance Management. Roles in these areas should also be better defined. For more information on the and management, see the Improvement Roadmap and Policy and Process Area Detail sections of this report.

Policy and Process Scores by Security Area

As with the section above, these scores can be used to identify areas for improvement and prioritize the order in which to address them.



Info-Tech Research Group

Addressing gaps in documentation and enforceme
more information on the specific steps you can tal

Assess process maturity across 7 areas of security. Determine which areas require the most improvement and use this report to investigate process improvement opportunities..

hat security is consistently meeting the organization's needs. For
s Area Detail sections of this report.

Recommended Actions Roadmap: Improve

Get a prioritized list of security areas requiring immediate attention. Use this to focus work effort and build improvements.

Prepared for:
Mike Buma, Strategy Analyst and Product Owner

powered by INFO~TECH RESEARCH GROUP

This section consolidates the high priority recommende prove on your biggest gaps and inconsistencies, and to address deficiencies in areas of greater importance.

URGENT — Urgency Score 10 / 10

Security Culture
Assessment

ACTION

Ensure that assessments of security awareness training uptake are conducted on at least an annual basis for the most critical security controls, and targeting the most critical user populations.

URGENT — Urgency Score 10 / 10

End User Devices Security
Deployment and Decommissioning

ACTION

Formalize and document this policy or process, then ensure accountability to achieve consistency.

URGENT — Urgency Score 10 / 10

Physical Security
Incorporation in Other Processes

ACTION

Formalize and document this policy or process, then ensure accountability to achieve consistency.

URGENT — Urgency Score 8 / 10

Host Security for Servers
Risk Analyis for Patches/Updates

ACTION

Formalize and document this policy or process, then ensure accountability to achieve consistency.

URGENT — Urgency Score 8 / 10

Security Culture
End User Evaluation

ACTION

Ensure that refresher training on key security awareness messages is completed on at least an annual basis. Consider more frequent training and awareness campaigns for the most critical security awareness messages.

HIGH — Urgency Score 6 / 10

Compliance Management
Accountability

ACTION

Clarify accountability and responsibility for compliance management, and communicate to affected stakeholders.

HIGH — Urgency Score 6 / 10

Vulnerability Management
Status

ACTION

Formalize and document vulnerability management processes, then ensure accountability to achieve consistency.

HIGH — Urgency Score 6 / 10

Vulnerability Management
Comprehensiveness

ACTION

Ensure that all aspects of security are included in vulnerability management processes to optimize vulnerability management.

HIGH — Urgency Score 6 / 10

Security Culture
Methods

ACTION

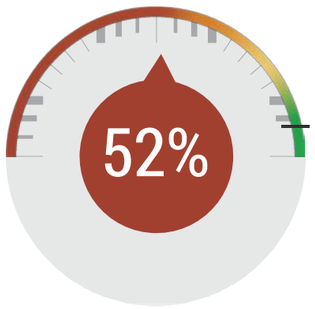
Ensure that new hire security awareness training is provided to all new staff within a reasonable timeframe post-hire. Focus on the most critical security messages to get the biggest bang for your training buck.

HIGH — Urgency Score 6 / 10

Security Culture
Foundation

ACTION

Ensure that assessments of security training uptake are conducted on at least an annual basis for the most critical security controls, and targeting the most critical systems.



Vulnerability Management Weighted Area Score: 3.1/6

Previous: 2.1/6

Vulnerability Management - Security Governance Areas

Vulnerability management is critical for establishing initial security configurations and maintaining a secure state over time. Use this report to understand and improve your vulnerability management capabilities.

QUESTION WEIGHT AND SIGNIFICANCE

Current Score Previous Score

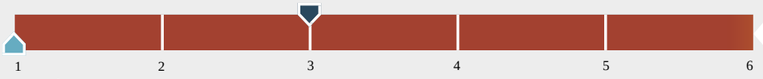
RECOMMENDED ACTIONS

Status

Please indicate the status of your vulnerability management process.

Vulnerability management provides organizations with visibility into, and processes for remediating, known technical vulnerabilities associated with current and planned technology implementations.

STATUS - Current Score **3/6** - Weight: High



Previous Score 1/6

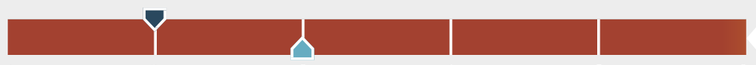
Formalize and document vulnerability management processes, then ensure accountability to achieve consistency.

Comprehensiveness

Is vulnerability management applied and enforced in all areas of security?

Vulnerability management activities must cover all aspects of security, or unnecessary residual risks will exist in the areas that have not been considered.

STATUS - Current Score **2/6** - Weight: Medium



Previous Score 3/6

Ensure that all aspects of security are included in vulnerability management processes to optimize vulnerability management.

Project Planning and Change Management

Are security considerations included in project planning and change management processes?

Vulnerability management activities must be part of all significant IT initiatives and changes, or unnecessary residual risks will exist.

STATUS - Current Score **3/6** - Weight: Medium

Previous Score 3/6

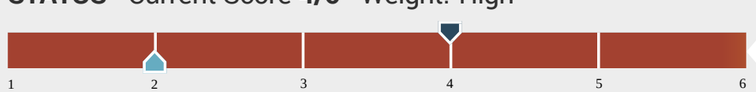
Expand the application of vulnerability management processes to a broader set of significant projects and changes.

Accountability

Have responsibility and accountability been clearly established for your vulnerability management process?

Without clear roles and responsibilities documented, vulnerability management processes run the risk of being ignored or circumvented.

STATUS - Current Score **4/6** - Weight: High



Previous Score 2/6

Clarify accountability and responsibility for vulnerability management, and communicate to affected stakeholders.

Evaluate the effectiveness of individual security governance areas.
For low scoring areas, follow recommended actions to start improvement efforts

Business Satisfaction and Alignment REPORT

PREPARED FOR:

Joe Computerguy
Computer Business Inc.

IT SECURITY DIAGNOSTIC PROGRAM
POWERED BY INFO-TECH RESEARCH GROUP

Lean42

INFO~TECH RESEARCH GROUP

TEST DOCUMENT

Business Satisfaction with IT Security

Computer Business Inc.

Business Responses Only

# of Employees	37
# of Responses	37
Response Rate	100.0%

powered by INFO-TECH RESEARCH GROUP

Business satisfaction is defined as confidence in important security areas and minimal friction for business processes.

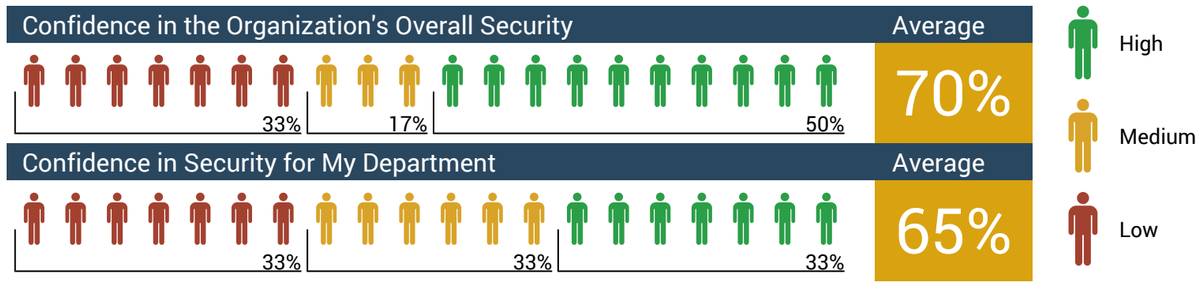
Security Importance and Confidence

Identify the business perspective on security importance and confidence at the department and organizational level. Low importance scores for "My Department" might reflect under-valuing their own day-to-day security practices. Similarly, low confidence scores might reveal hidden vulnerabilities (e.g., staff sharing passwords).

Importance and Confidence for Overall Security

Overall, how important is IT security to your organization/department?

Overall, how confident are you in the existing IT security practices for your organization/department?

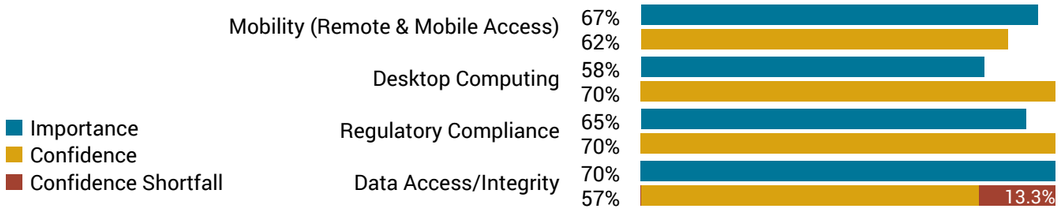


Importance vs. Confidence Detailed Breakdown

Target improvement efforts on areas with high Confidence Shortfalls (i.e., confidence lower than importance).

How important are IT security practices in these areas?

How confident are you in the existing IT security practices in these areas?



Security Friction

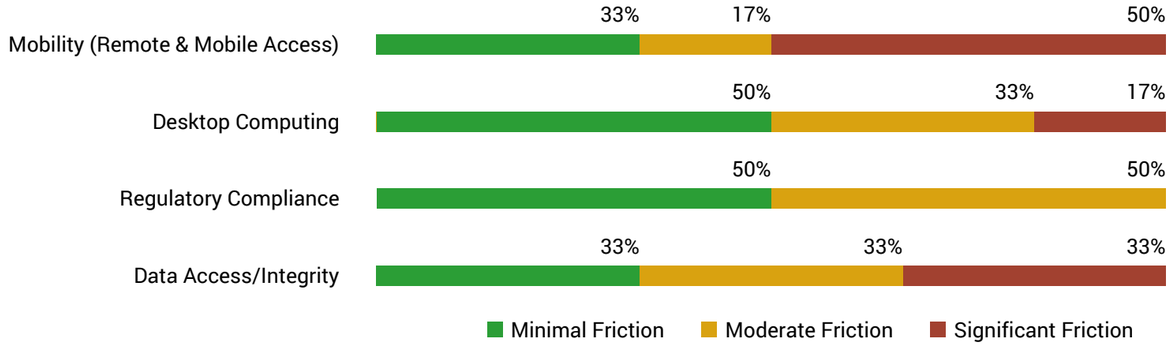
Address high friction areas with the business and modify security practices as necessary.

Security Friction Overall

Overall, how much friction do IT security practices create for business processes?

Security Friction Detailed Breakdown

How much do the IT security practices in these areas create friction for business processes?



Responsibility for Security Governance

Shared IT-business responsibility for security governance (e.g., risk analysis) leads to better alignment and greater understanding of risk tolerance, security priorities, and acceptable security practices.

Who should have responsibility for these IT security governance areas?

IT Satisfaction with IT Security

Computer Business Inc.

IT Responses Only

# of Employees	18
# of Responses	18
Response Rate	100.0%

powered by INFO-TECH RESEARCH GROUP

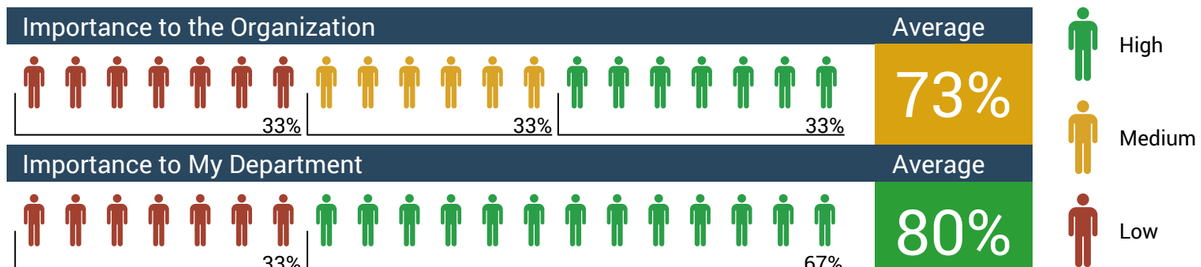
Business satisfaction is defined as confidence in important security areas and minimal friction for business processes.

Security Importance and Confidence

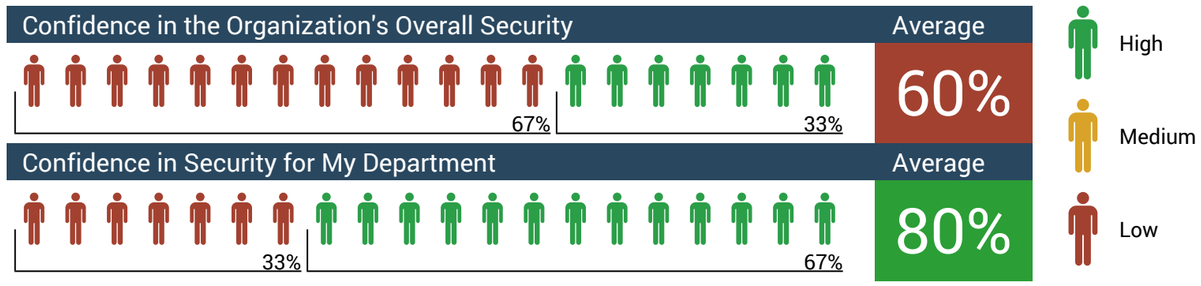
Identify the business perspective on security importance and confidence at the department and organizational level. Low importance scores for "My Department" might reflect under-valuing their own day-to-day security practices. Similarly, low confidence scores might reveal hidden vulnerabilities (e.g., staff sharing passwords).

Importance and Confidence for Overall Security

Overall, how important is IT security to your organization/department?



Overall, how confident are you in the existing IT security practices for your organization/department?

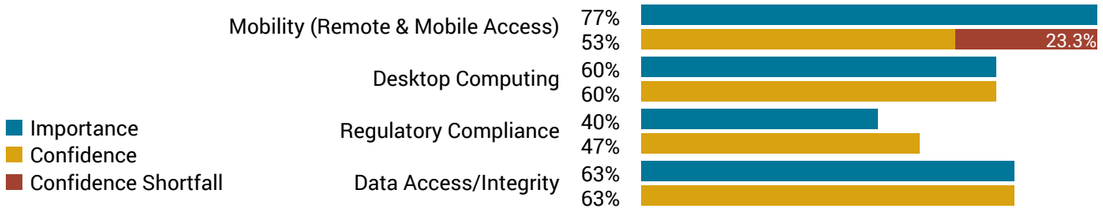


Importance vs. Confidence Detailed Breakdown

Target improvement efforts on areas with high Confidence Shortfalls (i.e., confidence lower than importance).

How important are IT security practices in these areas?

How confident are you in the existing IT security practices in these areas?



Security Friction

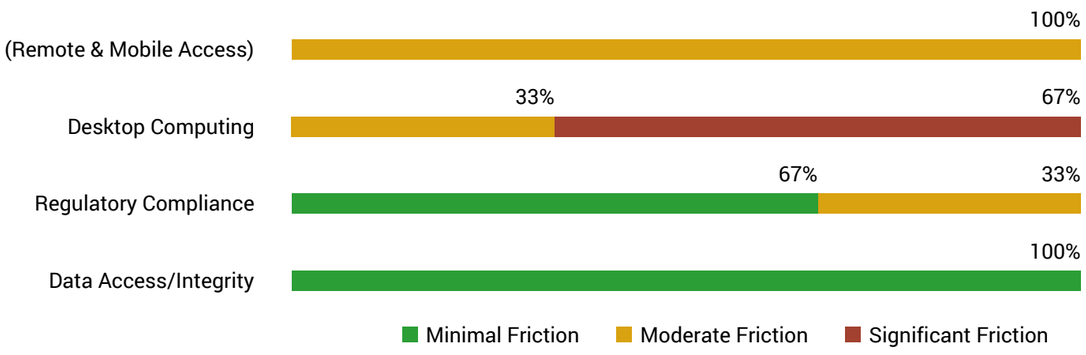
Address high friction areas with the business and modify security practices as necessary.

Security Friction Overall

Overall, how much friction do IT security practices create for business processes?

Security Friction Detailed Breakdown

How much do the IT security practices in these areas create friction for business processes?



Responsibility for Security Governance

Shared IT-business responsibility for security governance (e.g., risk analysis) leads to better alignment and greater understanding of risk tolerance, security priorities, and acceptable security practices.

Who should have responsibility for these IT security governance areas?

IT-Business Alignment

Computer Business Inc.

IT & Business Responses

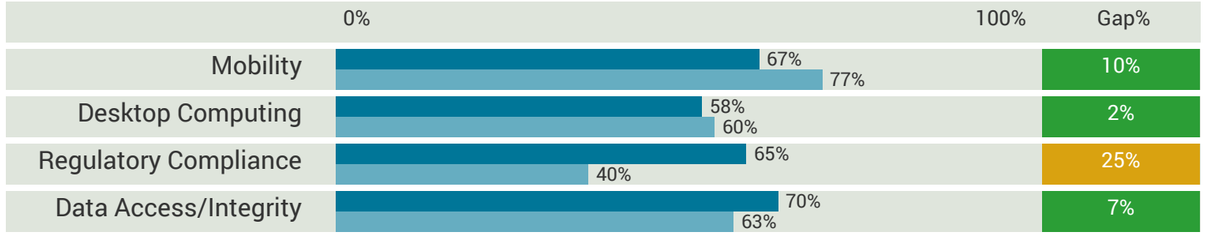
# of Employees	55
# of Responses	55
Response Rate	100.0%

powered by INFO~TECH RESEARCH GROUP

Identify gaps between IT and the business, and use that to drive alignment exercises.

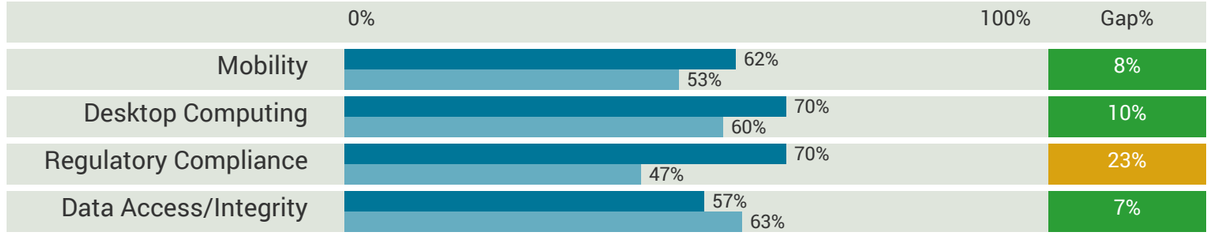
Security Importance

How important are IT security practices in these areas? Business's Response | IT's Response



Security Confidence

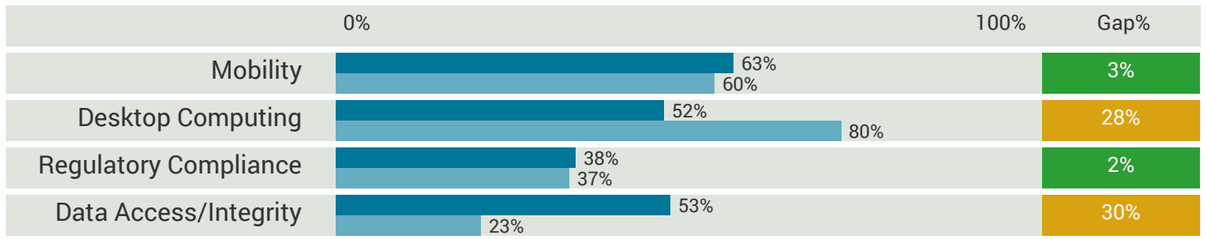
How confident are you in the existing IT security practices in these areas? Business's Response | IT's Response



GAP LEGEND | 0-15% Well-Aligned | 16-30% Review and Consider Alignment Exercise | 31+ % Conduct Alignment Exercise

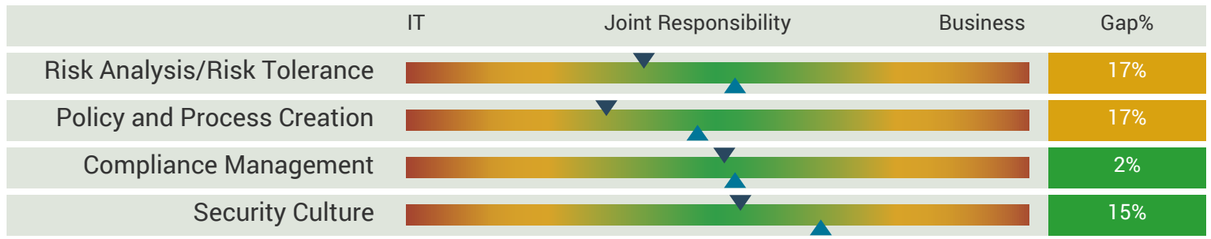
Security Friction

How much do the IT security practices in these areas create friction for business processes? Business's Response | IT's Response



Responsibility for Security Governance

Who should have responsibility for these IT security governance areas? ▲ IT ▼ Business



Follow These Steps to Close Gaps and Improve Satisfaction

1. **Meet with business users to explore scores that are misaligned** – e.g., are confidence gaps due to perception only or are concerns founded in sub-optimal security practices?

2. For importance and confidence gaps, **identify the root cause and review related practices.** For example, if mobility confidence is low, is the underlying concern protecting data on mobile devices or preventing malware attacks? Similarly, if mobility security has a high importance score due to data concerns, then also review overall data access/integrity security concerns.

3. For security satisfaction low scores and gaps, **identify the specific practices that are deemed too restrictive or cumbersome, and the underlying causes of dissatisfaction.** For example, if remote access friction is actually due to usability issues with the VPN client and not security policies, then the issue may be solved by exploring alternative VPN client solutions. In other cases, it may be necessary to re-align end-user perspectives on security requirements.

4. For governance responsibility gaps, **determine the potential points of friction (e.g., time commitment) to move towards joint responsibility** so you can have an informed discussion of what is appropriate. For example, joint responsibility does not mean identical time commitments. In risk analysis, for example, it's still IT's responsibility to identify and present risks and mitigation options; the business role is to provide feedback on risk tolerance.

5. **Leverage Info-Tech's Security Effectiveness reports** for a deeper review of security practices.

End User Devices

Security Effectiveness Report

IT SECURITY
DIAGNOSTIC PROGRAM
POWERED BY INFO-TECH RESEARCH GROUP

Lean42

PREPARED FOR:

Mike Buma
Info-Tech Research Group

INFO~TECH
RESEARCH GROUP

End User Devices Security Effectiveness Report

Info-Tech Research Group

Prepared for:
Mike Buma

powered by INFO~TECH RESEARCH GROUP

OVERALL EFFECTIVENESS SCORE

These scores reflect your team's view of End User Devices security effectiveness. The overall score gives a high level sense of where you're at in this area, while the policy and process and technology scores summarize your team's responses in these subcategories.

OVERALL POLICY AND PROCESS EFFECTIVENESS SCORE

OVERALL

OVERALL TECHNOLOGY EFFECTIVENESS SCORE

MOST EFFECTIVE POLICIES AND PROCESSES

According to your team, these policies and processes are your most effective. Effectiveness scores reflect confidence in threat identification and prevention and the ability to minimize adverse impact on end user experience.

1	Device standards defined	Effectiveness Score	80%	
		Confidence: **78%**	Impact: **81%**	
2	Desktop/laptop standards defined	Effectiveness Score	79%	
		Confidence: **76%**	Impact: **81%**	
3	Audit deployment practices	Effectiveness Score	61%	
		Confidence: **61%**	Impact: **61%**	

LEAST EFFECTIVE POLICIES AND PROCESSES

According to your team, these End User Devices devices policies and processes are your least effective.

Deployment/ decommissioning checklist	Effectiveness Score	33%	
	Confidence: **39%**	Impact: **28%**	
Audit deployed devices	Effectiveness Score	35%	
	Confidence: **37%**	Impact: **33%**	
BYOD policies	Effectiveness Score	60%	
	Confidence: **54%**	Impact: **67%**	

TEAM ALIGNMENT

This section shows the areas in which your team is most closely aligned and most greatly divergent.

Most Aligned	Gap
Patch/update risk analysis	2%
BYOD policies	2%
Device standards defined	2%

Least Aligned	Gap
Application Whitelisting	76%
Patch Management	37%
Personal/Client Firewalls	37%

MOST EFFECTIVE TECHNOLOGIES

According to your team, these technologies are your most effective. Effectiveness scores reflect confidence in threat identification and prevention and the ability to minimize adverse impact on end user experience.

1	Endpoint Encryption	Effectiveness Score	81%	
		Confidence: **83%**	Impact: **79%**	
2	Patch Management	Effectiveness Score	79%	
		Confidence: **83%**	Impact: **75%**	
3	Endpoint Anti-Malware	Effectiveness Score	73%	
		Confidence: **75%**	Impact: **71%**	

LEAST EFFECTIVE TECHNOLOGIES

According to your team, these End User Devices technologies are your least effective.

Application Whitelisting	Effectiveness Score	40%	
	Confidence: **42%**	Impact: **38%**	
Personal/Client Firewalls	Effectiveness Score	69%	
	Confidence: **67%**	Impact: **71%**	

Policy and Process

Info-Tech Research Group

Prepared for:
Mike Buma

powered by INFO~TECH RESEARCH GROUP

Policy and Process Effectiveness Score

This score summarizes your team's opinions on End User Devices security policies and processes. It is a high level indicator of where you're at in this area.

Confidence and impact are key indicators of security effectiveness. The overall effectiveness score is determined by the arithmetic mean of your team's policy and process confidence and impact responses.

Security Confidence
The degree of confidence expressed by relevant IT personnel that policies and processes in this area are preventing and identifying threats.

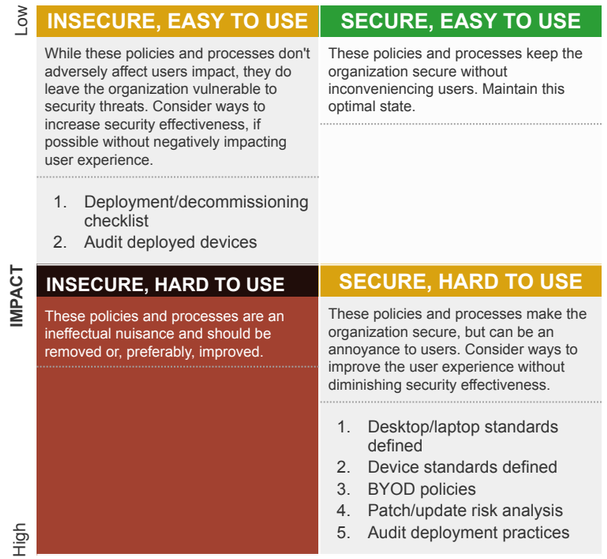
Adverse Impact
The level of adverse impact on end user experience that relevant IT personnel believe is caused by policies and processes in this area.

Policy and Process Drivers of End User Devices Security Effectiveness

Successful security depends on having effective policies and processes. Use this section to understand your team's perspective on which policies are working well and which aren't.

Effectiveness Score		Policy or Process	Evaluation Criteria: Confidence Respondents by % and #	Reponse Average	Previous Average	Evaluation Criteria: Impact Respondents by % and #	Response Average	Previous Average
79%	1	**Desktop/laptop standards defined** Internal security standards defined for each desktop/ laptop platform.	22% [2] 22% [2] 56% [5]	76%	56%	11% [1] 11% [1] 78% [7]	81%	38%
80%	2	**Device standards defined** Internal security standards defined for each tablet or smartphone platform.	11% [1] 33% [3] 56% [5]	78%	63%	11% [1] 11% [1] 78% [7]	81%	35%
33%	3	**Deployment/decommissioning checklist** Complete a security checklist as part of deployment and decommissioning processes.	67% [6] 11% [1] 22% [2]	39%	65%	89% [8] 11% [1] 0% [0]	28%	52%
35%	4	**Audit deployed devices** Audit deployed devices to ensure they still meet requirements.	67% [6] 11% [1] 22% [2]	37%	67%	78% [7] 11% [1] 11% [1]	33%	54%
60%	5	**BYOD policies** Determine acceptable use of employee-owned devices.	11% [1] 78% [7] 11% [1]	54%	46%	22% [2] 33% [3] 44% [4]	67%	63%
61%	6	**Patch/update risk analysis** Perform a risk analysis prior to deploying patches/updates.	11% [1] 78% [7] 11% [1]	63%	42%	11% [1] 78% [7] 11% [1]	59%	50%
61%	7	**Audit deployment practices** Audit device deployment practices to ensure they are being followed.	11% [1] 56% [5] 33% [3]	61%	40%	22% [2] 44% [4] 33% [3]	61%	54%

■ Response of 1 or 2 (low/bad) ■ Response of 3 or 4 (medium/moderate) ■ Response of 5 or 6 (high/good)



Policy and Process Execution Consistency - Team Alignment

Policies and processes aren't fully effective unless they're documented, enforced, reviewed, and optimized. Use this section to ensure your team is on the same page in terms of your policies and process status.

Question: "To what extent are the following policies in place and enforced?"

Response of one or two (respondents believe policy or process has low maturity)
Response of three or four (respondents believe policy or process has moderate maturity)
Response of five or six (respondents believe policy or process has high maturity)

1 Not in place
2 Informal policy in place, inconsistently applied
3 Informal policy in place, consistently applied
4 Formal policy in place, inconsistently applied
5 Formal policy in place, consistently applied
6 Formal policy, consistently applied, and has been reviewed and optimized

The ideal outcome for this section would be perfect consensus among respondents. If policy and process requirements aren't known, they can't be followed through on or effectively enforced. But simply being aware of a policy or process is not enough, ideally the entire team should have a stake in review and optimization.

	Policy and Process	Respondents by % and #	Response Average	Previous Average	Policy and Process Status - Team Alignment
1	**Desktop/laptop standards defined** Internal security standards defined for each desktop/laptop platform.	67% [6] 33% [3] 0% [0]	37%	69%	IT Staff Avg. CSO CIO
2	**Device standards defined** Internal security standards defined for each tablet or smartphone platform.	22% [2] 56% [5] 22% [2]	56%	61%	IT Staff Avg. CSO CIO
3	**Deployment/decommissioning checklist** Complete a security checklist as part of deployment and decommissioning processes.	0% [0] 67% [6] 33% [3]	70%	69%	IT Staff Avg. CSO CIO
4	**Audit deployed devices** Audit deployed devices to ensure they still meet requirements.	11% [1] 56% [5] 33% [3]	63%	67%	IT Staff Avg. CSO CIO
5	**BYOD policies** Determine acceptable use of employee-owned devices.	11% [1] 44% [4] 44% [4]	74%	73%	IT Staff Avg. CSO CIO
6	**Patch/update risk analysis** Perform a risk analysis prior to deploying patches/ updates.	11% [1] 33% [3] 56% [5]	78%	81%	IT Staff Avg. CSO CIO
7	**Audit deployment practices** Audit device deployment practices to ensure they are being followed.	11% [1] 67% [6] 22% [2]	57%	67%	IT Staff Avg. CSO CIO

BUILD A DATA-DRIVEN IT STRATEGY

Make Informed IT Decisions by Starting Your Diagnostic Program Today!

https://lean42.com/lean-packages/it-diagnostics/

Use our proven Diagnostocs Program - the simplest way to collect the data you need, turn it into actionable insights, and communicate with stakeholders across the organization.

BUILD A DATA-DRIVEN IT STRATEGY

Use IT assessments to make data-driven IT strategy your most effective weapon.

CIO BUSINESS VISION

CIO-CEO ALIGNMENT DIAGNOSTIC

ASSESS CORE IT PROCESSES

IT STAFFING ASSESSMENT

APPLICATION PORTFOLIO ASSESSMENT

END USER SATISFACTION PROGRAM

PROJECT PORTFOLIO MANAGEMENT DIAGNOSTIC PROGRAM

IT SECURITY DIAGNOSTIC PROGRAM

DATA QUALITY SCORECARD

https://lean42.com/lean-packages/it-diagnostics/