The background of the entire page is a dark blue-tinted image of a modern office interior. In the foreground, several people are silhouetted against a large window. They appear to be in a meeting, with some sitting at a long table and one person standing and leaning over. The window looks out onto a city skyline with various skyscrapers. The overall atmosphere is professional and high-tech.

# Security Management Scorecard

Collect the Data You Need to Effectively Manage IT Security

# Your Journey Starts Here.

**Understand Your Security Management Strengths & Weaknesses**

**Evaluate Performance and Required Next Steps by Security Area**

**Build a Security Improvement Roadmap**

The following report is a sample of what you will receive after completing the Security Management Scorecard. Each report is customized to the individual organization highlighting the IT Security Team's most pressing needs.

Complete the diagnostic program to get the data you need to start your security management journey.



# Security Management Scorecard Copy: [Inside the Report](#)

---



## 1 Understand Your Security Management Strengths & Weaknesses

Once a year, take a step back from day-to-day security operations and look at the big picture.

Measure your security management practices against industry standard best practices

Build your framework for managing & improving security practices over the long term.



## 2 Evaluate Performance and Required Next Steps by Security Area

Identify areas for improvement, and justify allocation of resources toward these goals.

Communicate current strengths, and use year over year comparisons to measure long term progress.

Measure success in terms of meeting industry standard best practices.



## 3 Build a Security Improvement Roadmap

Cut through the noise: uncover the processes that really matter in building your world-class IT security function.

Align your team behind achieving your vision, communicating the rationale behind your decisions.

Prioritize quick wins to show your stakeholders that rapid improvement is a priority.

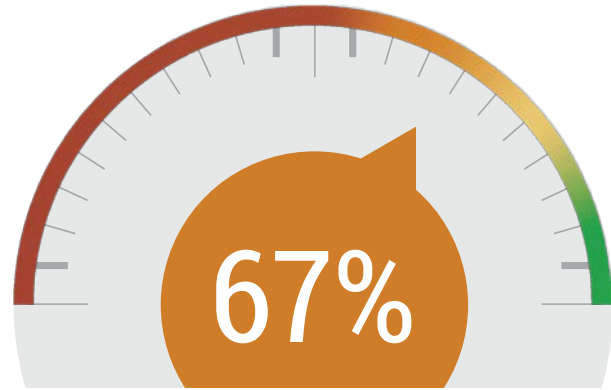
# Governance & Management SCORECARD

Fill out by yourself or with your team.

**PREPARED FOR:**

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

## Overall Maturity Score

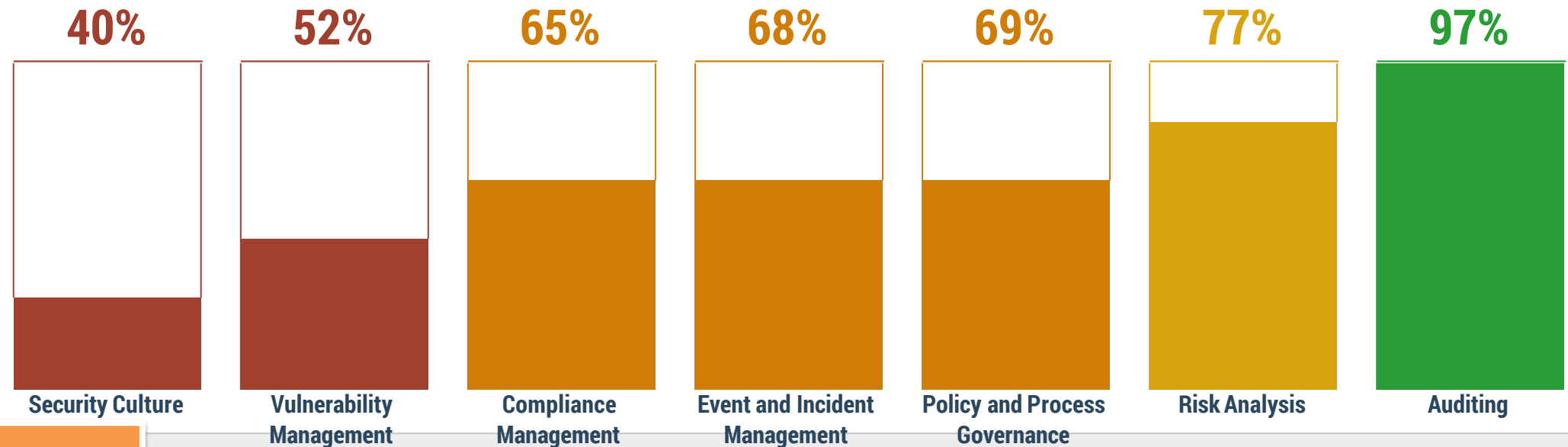


Measuring and communicating success in IT Security can be difficult. This score is a summary indicator of where you're at in relation to industry standard best practices.

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..

## Scores by Governance and Management Area

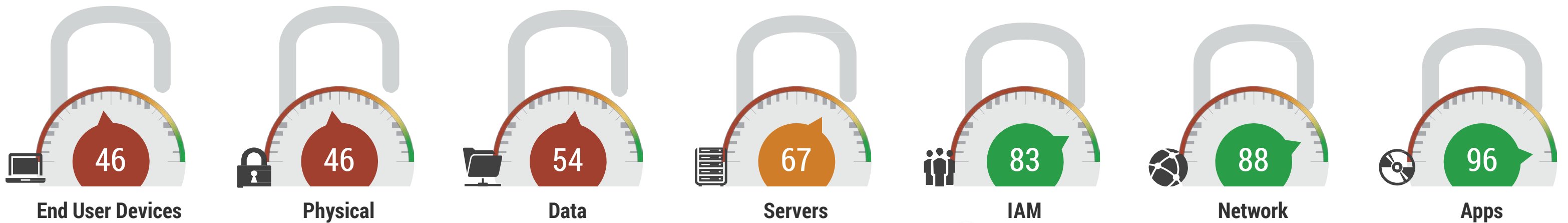
Use this information to identify and prioritize opportunities for improvement.



Security 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 enforcement more information on the specific steps you can take

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

that security is consistently meeting the organization's needs. For more information on the specific steps you can take, see the Policy and Process Area Detail sections of this report.

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

This section consolidates the high priority recommended actions to address deficiencies in areas of greater importance.


Improve on your biggest gaps and inconsistencies, and to

Urgency Score  
**URGENT 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.

Urgency Score  
**URGENT 10 / 10**

 **End User Devices Security**  
Deployment and Decommissioning


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

Urgency Score  
**URGENT 10 / 10**

 **Physical Security**  
Incorporation in Other Processes


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

Urgency Score  
**URGENT 8 / 10**

 **Host Security for Servers**  
Risk Analysis for Patches/Updates


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

Urgency Score  
**URGENT 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.

Urgency Score  
**HIGH 6 / 10**

 **Compliance Management**  
Accountability


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

Urgency Score  
**HIGH 6 / 10**

 **Vulnerability Management**  
Status


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

Urgency Score  
**HIGH 6 / 10**

 **Vulnerability Management**  
Comprehensiveness


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

Urgency Score  
**HIGH 6 / 10**

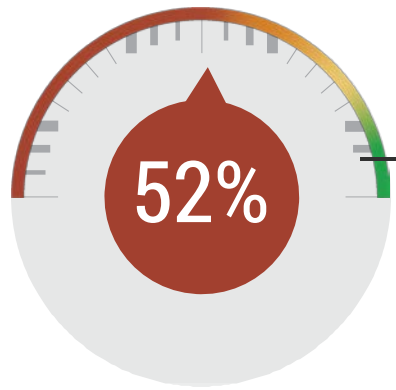
 **Security Culture**  
Methods

**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.

Urgency Score  
**HIGH 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**

1 of 5

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

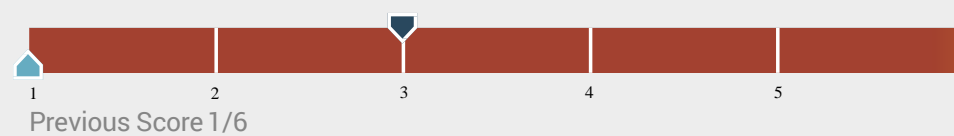
**RECOMMENDED ACTIONS**

**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**



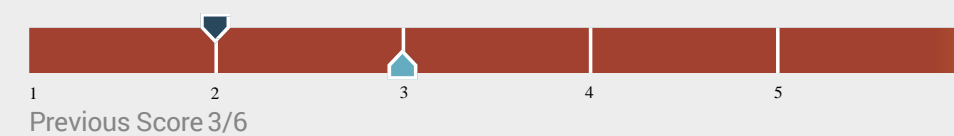
Formalize and document vulnerability management processes, then ensure accountability to achieve consistency.

**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**



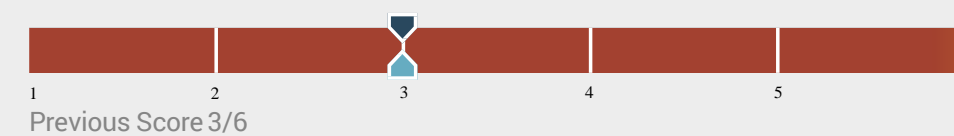
Ensure that all aspects of security are included in vulnerability management processes to optimize vulnerability management.

**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**



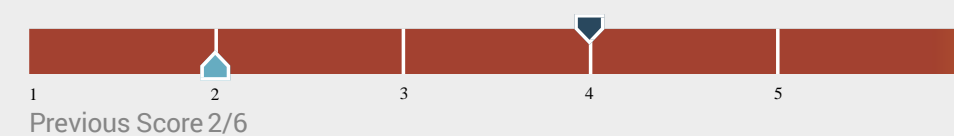
Expand the application of vulnerability management processes to a broader set of significant projects and changes.

**Accountability**

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

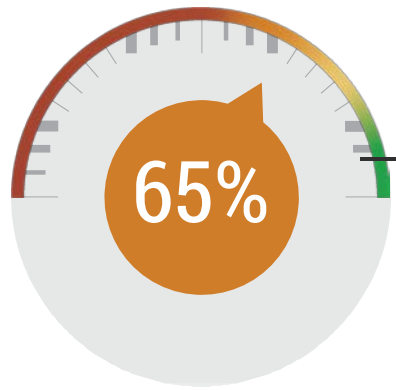
Without clear roles and responsibilities documented, vulnerability management processes run the risk of being ignored or circumvented.

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



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



## Compliance Management Weighted Area Score: 3.9/6

Previous: 4.5/6

### Compliance Management - Security Governance Areas

2 of 5

Regulatory and policy compliance are key elements of many organizations' information security programs. This report demonstrates the state of your compliance management efforts.

#### QUESTION WEIGHT AND SIGNIFICANCE

Current Score Previous Score

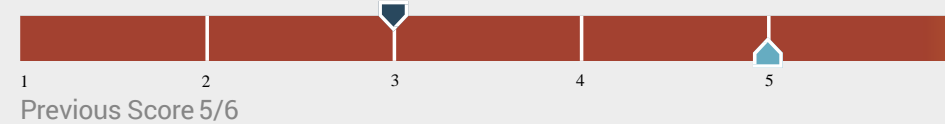
#### RECOMMENDED ACTIONS

##### Accountability

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

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

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



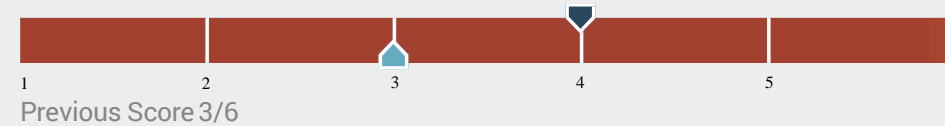
Clarify accountability and responsibility for compliance management, and communicate to affected stakeholders.

##### Status

**Please indicate the status of your compliance management process.**

Formality of supporting processes is critical to establishing and maintaining compliance with regulatory and policy requirements.

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



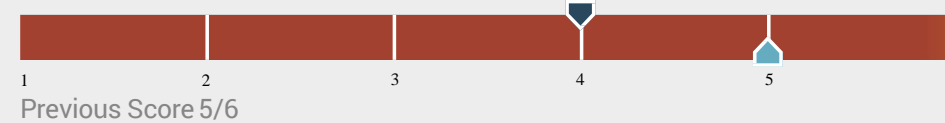
Ensure accountability and enforcement to achieve consistency in your compliance management processes.

##### Exceptions

**Are explicitly approved exceptions audited, monitored, and reported?**

Compliance exceptions must be documented and managed, or else the organization risks falling into a non-compliant state.

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



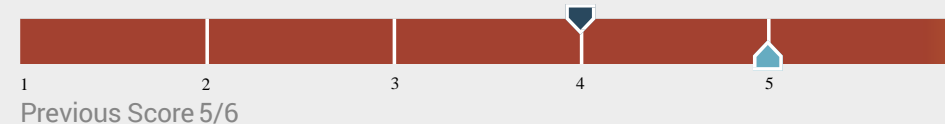
Ensure that compliance exception handling processes are formalized, and expand to ensure that all staff are aware of the exception process.

##### Promotion and Enforcement

**Is compliance promoted and enforced?**

A culture of compliance begins with promotion of the compliance obligations, and relies heavily on enforcement mechanisms to detect and remediate compliance violations.

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



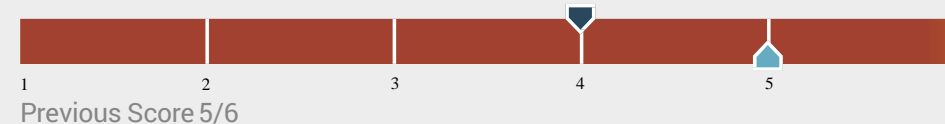
Formalize compliance enforcement protocols so reported violations can be handled in a consistent manner.

##### Issues Investigation

**Are issues investigated to prevent further offenses?**

Addressing compliance violations as one-off problems is only half of the story; seek out process-related and other systemic breakdowns to ensure that issues don't propagate.

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



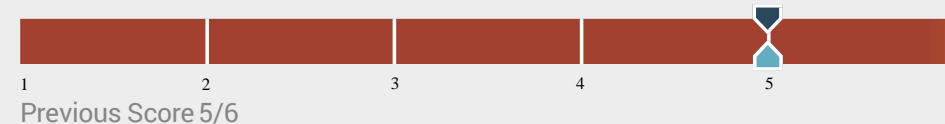
Formalize and expand your capabilities for investigating compliance violations.

##### Communication

**Are compliance requirements communicated to relevant staff?**

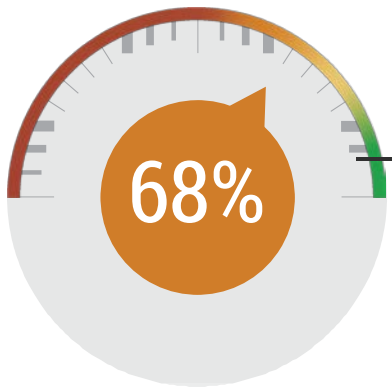
Compliance with regulation and policy is challenging if you haven't communicated those requirements; ensure all those with a need to know have been informed of their obligations.

**STATUS - Current Score 5/6 - Weight: Medium**



Ensure that compliance communication plans include broad communications for general staff and more specific elements targeted at those most affected by compliance requirements.





**Event and Incident Management Weighted Area Score: 4.1/6**

Previous: 1.8/6

**Event and Incident Management - Security Governance Areas**

3 of 5

Event and incident management enable proactive and rapid reaction responses to potential and actual threats to information security. Use this report to focus on the key aspects of your response processes.

**QUESTION WEIGHT AND SIGNIFICANCE**

Current Score Previous Score

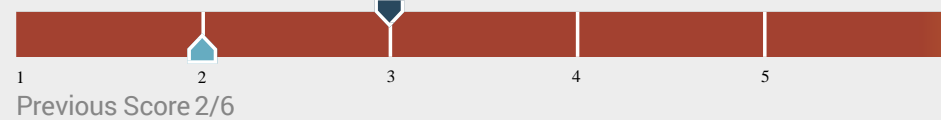
**RECOMMENDED ACTIONS**

**Event Comprehensiveness**

**Does your event monitoring include all areas of security?**

Event monitoring is needed for all areas of IT security, otherwise blind spots will exist that introduce unnecessary risk.

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



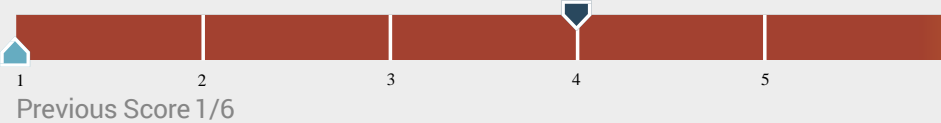
Ensure that all aspects of security are included in event monitoring processes to optimize event monitoring.

**Status**

**Please indicate the status of your event and incident management process.**

Event and incident management process formality provides the basis for organizational confidence that attacks and other security events can be detected and responded to in a timely and thorough manner.

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



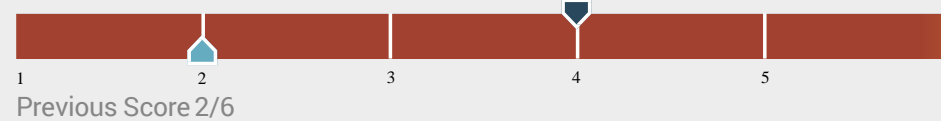
Ensure accountability and enforcement to achieve consistency in your event/incident management processes.

**Event Accountability**

**Have responsibility and accountability been clearly established for your event monitoring?**

Without clear roles and responsibilities, event monitoring often is overlooked in favour of other operational duties; if event monitoring isn't done consistently, incidents may be overlooked.

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



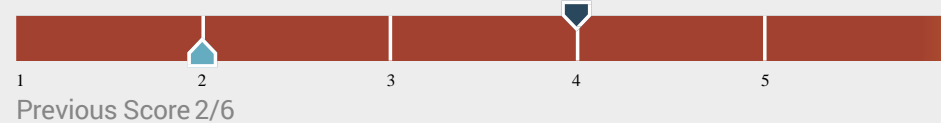
Clarify accountability and responsibility for event monitoring processes, and communicate to affected stakeholders.

**Incident Comprehensiveness**

**Does your incident management include all areas of security?**

Incident management is needed for all areas of IT security, otherwise unnecessary risk will result from inconsistent handling of escalated incidents.

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



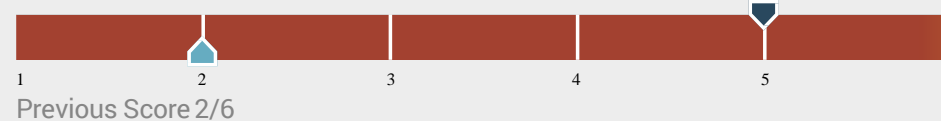
Ensure that all aspects of security are included in incident monitoring processes to optimize incident management.

**Incident Accountability**

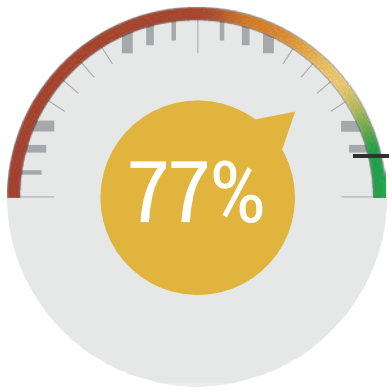
**Have responsibility and accountability been clearly established for your incident management?**

Without clear roles and responsibilities, incident handling can be confused and inconsistent, resulting in prolonged response times and elevated risk.

**STATUS - Current Score 5/6 - Weight: High**



Ensure that incident management processes roles and responsibilities have been communicated to affected stakeholders in all situations.



## Risk Analysis Weighted Area Score: 4.6/6

Previous: 2.3/6

### Risk Analysis - Security Governance Areas

4 of 5

Appropriate security measures start with risk analysis to understand the threats, potential impact, and business tolerance for risk. Use this report to understand your risk analysis score and to improve process maturity and comprehensiveness in this area.

#### QUESTION WEIGHT AND SIGNIFICANCE

Current Score Previous Score

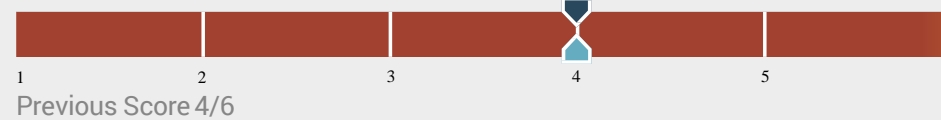
#### RECOMMENDED ACTIONS

##### Comprehensiveness

##### Are all security areas covered in your risk analysis?

Risk analysis activities must cover all aspects of security, or unnecessary residual risks and/or unrealized opportunities will exist in the areas that have not been considered.

STATUS - Current Score 4/6 - Weight: Medium



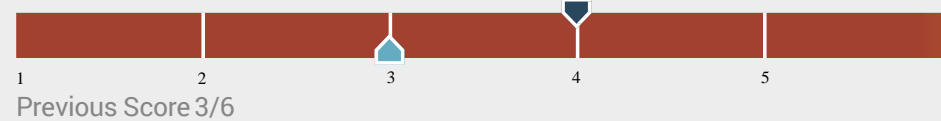
Ensure that all aspects of security are included in risk analysis to optimize risk management outcomes.

##### Projects

##### Is risk analysis conducted for all significant projects?

Risk analysis activities must cover all significant IT initiatives, or unnecessary residual risks and/or unrealized opportunities will exist for the projects that have not been considered.

STATUS - Current Score 4/6 - Weight: Medium



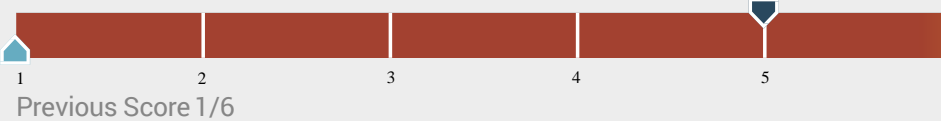
Expand the application of risk analysis to a broader set of significant projects.

##### Status

##### Please indicate the status of your risk analysis process.

Risk analysis process formality underpins effective risk management decision making. Optimized risk analysis turns risk from a threat into an opportunity.

STATUS - Current Score 5/6 - Weight: High



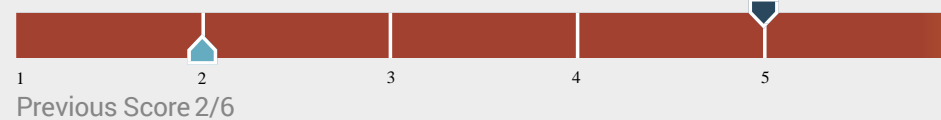
Conduct periodic reviews to ensure risk analysis is meeting organizational needs and has been optimized.

##### Accountability

##### Have responsibility and accountability been clearly established for your risk analysis process?

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

STATUS - Current Score 5/6 - Weight: High



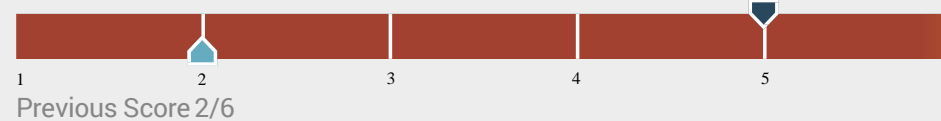
Ensure that risk analysis roles and responsibilities have been communicated to affected stakeholders in all situations.

##### Communication

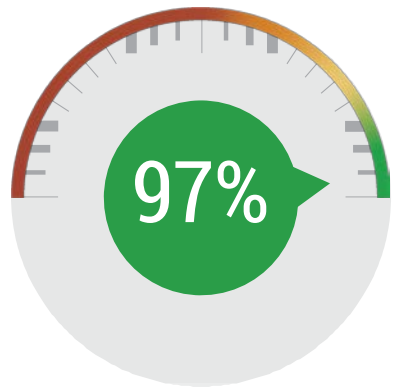
##### Are risk analysis outcomes clearly communicated to project teams for all significant projects?

Risk analysis outcomes (acceptance, mitigation) must be communicated to project team members if appropriate risk-based controls are to be implemented.

STATUS - Current Score 5/6 - Weight: Low



Expand the communication of risk analysis decisions to include all significant project teams.



**Auditing Weighted Area Score: 5.8/6**

Previous: 3.3/6

### Auditing - Security Governance Areas

5 of 5

A solid audit program is key to ensuring that information security policies and processes are being followed across the organization. This report will help you to focus on improvements in your security audit program.

#### QUESTION WEIGHT AND SIGNIFICANCE

Current Score Previous Score

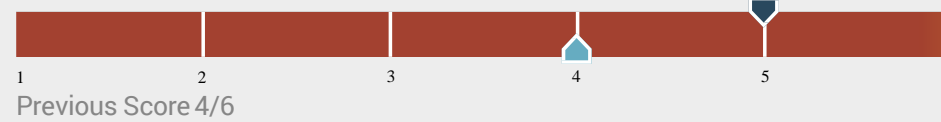
#### RECOMMENDED ACTIONS

##### Frequency

**How frequently do you audit for compliance with your security policies and processes?**

Audit frequency matters: ensure that compliance with critical processes is audited on a schedule that balances risk to the organization against the costs of the audit.

**STATUS - Current Score 5/6 - Weight: Medium**



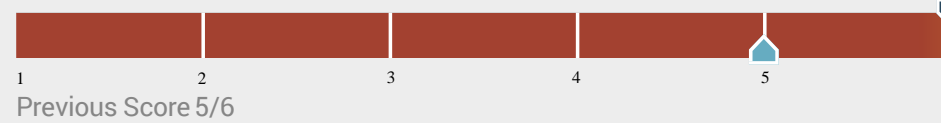
Ensure that the audit frequency is valuable to the organization, and consider reducing the audit frequency for less critical security policies.

##### Status

**Please indicate the status of your auditing process.**

Audit process formality provides the basis for organizational confidence that policies and processes are being followed properly.

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



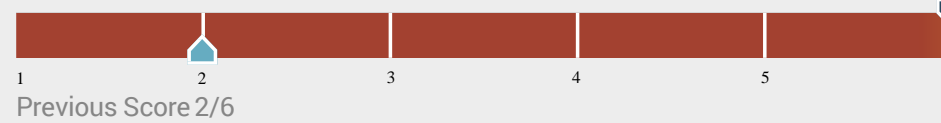
Best practices are in place for your auditing. Maintain optimal status through periodic reviews and continued enforcement.

##### Comprehensiveness

**Do your audits cover all areas of security?**

Audit processes must exist for activities across the full range of security areas, or residual risk will be higher than necessary.

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



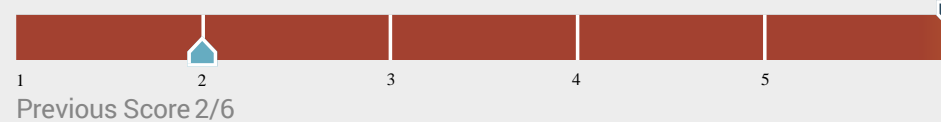
Best practices are being followed for auditing. Maintain optimal status through periodic reviews and continued enforcement.

##### Accountability

**Have responsibility and accountability been clearly established for your auditing process?**

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

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



Best practices are being followed for auditing roles and responsibilities. Maintain optimal status through periodic reviews and continued enforcement.



## Security Culture: End User

**No matter how good your security controls, the weakest link will always be your people.**

Creating a security culture through training and assessment is the most effective way to mitigate human risk. Info-Tech has identified four core elements of successful security awareness training for end users:

---

Methods

---

Scope

---

Frequency

---

Foundation

---



## Security Culture: IT

**Security ultimately depends on IT**

Whether the task is instituting security controls, training and assessing end users, or executing on the organization's risk tolerance decisions, security hinges in large part on the knowledge and diligence of IT staff. Info-Tech has identified four core areas of IT responsibility that are crucial to creating a culture of security:

---

Expertise

---

Assessment

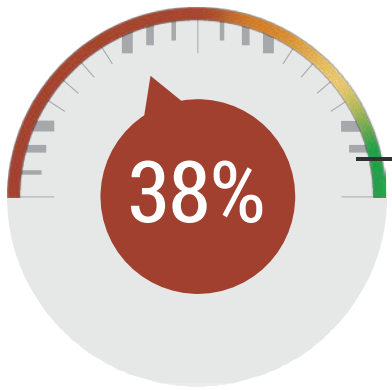
---

End User Evaluation

---

Knowledge Transfer

---



**Security Culture - End User**  
**Weighted Area Score: 2.3/6**

Previous: 3.9/6

Regardless of the security controls in place, users themselves represent a significant risk to information security. A strong security culture can mitigate this risk. This report shows the state of your efforts to foster a security culture among business users, the non-IT staff whose everyday actions may - most often through no malicious intent - create vulnerabilities and vectors for attack. Use the "recommended action" items to improve your security awareness training and address gaps in your process.

**Frequency**

Frequency matters: security awareness messages benefit from repetition, and in some cases frequent repetition.

**Methods**

Not everyone learns the same way, and some messages bear repeating; using multiple methods of delivering awareness and training materials will optimize outcomes.

**Foundation**

To meet the organization's expectations for security behavior, new hires must be provided with security awareness training - ideally before system access is granted.

**Scope**

Awareness training must cover activities across the full range of security areas, or residual risk will be higher than necessary.

"How often is security training provided to existing staff?"

Weight: Medium - Current Score 1/6

Previous Score 3/6

**RECOMMENDED 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.

Current Score

Previous Score

"Do you use a variety of methods in your security awareness training?"

Weight: Low - Current Score 2/6

Previous Score 1/6

**RECOMMENDED ACTION:** Ensure that a variety of methods are used to reach a wider population of users with diverse learning styles.

"Is security awareness training provided to new staff?"

Weight: Medium - Current Score 2/6

Previous Score 6/6

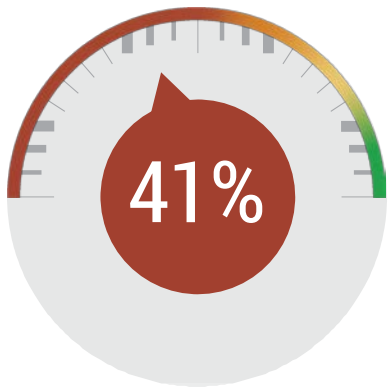
**RECOMMENDED ACTION:** Ensure that new hire security awareness training is provided to all new staff within a reasonable timeframe post-hire. Focus on the most critical security messages to get the biggest bang for your training buck.

"Does your security awareness training cover IAM, data, application, physical, and end user devices security?"

Weight: Medium - Current Score 4/6

Previous Score 4/6

**RECOMMENDED ACTION:** Ensure that all aspects of security are included in security awareness training materials to optimize security awareness training.



**Security Culture - IT Weighted Area Score: 2.5/6**

Previous: 2.5/6

Creating a culture of security depends in large part on the knowledge and diligence of IT personnel. This report shows where your IT personnel are at in terms of four areas of responsibility and accountability that are crucial to creating a culture of security. Use the "recommended action" items to improve your security awareness training and address gaps in your process.

“Do you assess the effectiveness of end user training through regular testing and follow up with users who fail these tests?”

Weight: High - Current Score 1/6

Previous Score 1/6

**RECOMMENDED 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.

### End User Evaluation

Testing is critical for reinforcing awareness training messages and ensuring that you can identify and remediate situations where the messages have not been internalized.

Current Score Previous Score

“Is special security training for system administrators, database administrators, network administrators, and application developers assessed and the results of these assessments followed up on?”

Weight: High - Current Score 3/6

Previous Score 4/6

**RECOMMENDED 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.

### Assessment

To maximize the benefit of specialized security training, assessment is key. The best things to assess are the system or code artifacts themselves.

Current Score Previous Score

“Have responsibility and accountability been clearly established for your security awareness training?”

Weight: High - Current Score 3/6

Previous Score 3/6

**RECOMMENDED ACTION:** Establish and document responsibility and accountability for security awareness training using a RACI chart.

### Knowledge Transfer

Without clear roles and responsibilities documented, security awareness training processes run the risk of being ignored or back-burnered.

Current Score Previous Score

“How often do your system administrators, database administrators, network administrators, and application developers get special security training?”

Weight: Medium - Current Score 3/6

Previous Score 2/6

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

### Expertise

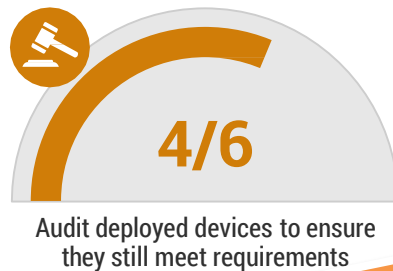
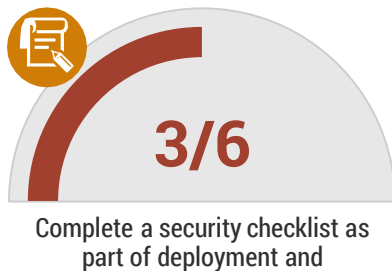
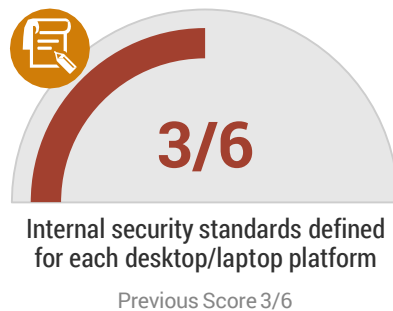
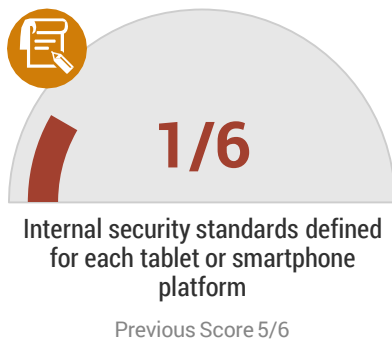
Specialized security training for IT staff is a necessity for secure development and operations.

Current Score Previous Score

End user devices, unlike servers, must retain flexibility to operate in support of users' diverse needs; this creates opportunities for malware to be introduced into the organization.

## Current Scores

"To what extent are the following policies and processes in place for End User Devices Security?"



Assess process maturity of individual security areas. Determine which processes you are missing or have not formalized.

### How to Improve

Use these action items to close the gaps in your core End User Devices Security policies and processes.

#### Recommended Actions

- 1 Document the Process:** Formalize and document this policy or process, then ensure accountability to achieve consistency.
- 2 Ensure enforcement:** Ensure accountability and enforcement to achieve consistency in this policy or process.
- 3 Conduct Reviews:** Conduct periodic reviews to ensure this policy or process is meeting organizational needs and has been optimized.

Get a list of recommendations for improvement. Begin taking action in key areas and optimizing policies & processes as needed.

### How to Optimize

Use the following checklist to ensure that all your End User Devices Security policies and processes are formalized, documented, enforced, and reviewed.

Policies and Processes	Optimized
Internal security standards defined for each tablet or smartphone platform	<input type="checkbox"/>
Internal security standards defined for each desktop/laptop platform	<input type="checkbox"/>
Complete a security checklist as part of deployment and decommissioning processes	<input type="checkbox"/>
Audit deployed devices to ensure they still meet requirements	<input type="checkbox"/>
BYOD policies	<input type="checkbox"/>
Perform a risk analysis prior to deploying patches/updates	<input type="checkbox"/>
Audit device deployment practices to ensure they are being followed	<input type="checkbox"/>

### Accountability

Establishing who is accountable for each policy and process is important for enforcement and quality control.

Internal security standards defined for each tablet or smartphone platform	No one - Assign Accountability
Internal security standards defined for each desktop/laptop platform	Bob Datacrunch
Complete a security checklist as part of deployment and decommissioning processes	No one - Assign Accountability
Audit deployed devices to ensure they still meet requirements	Joe Computerguy

See which processes are lacking clear accountability. Assign accountability against key processes.



Even when other people, process, and technology controls are in place, physical security breakdowns can lead to information risk. Ensure that your data and systems are secure against "low tech" physical security breaches.

## Current Scores

"To what extent are the following policies and processes in place for Physical Security?"



Visitor/guest registration and access policies

Previous Score 4/6



Before/after hours access policies

Previous Score 1/6



Incorporate physical security considerations into other processes

Previous Score 5/6



Audit physical security practices to ensure they are being followed

Previous Score 1/6

### How to Improve

Use these action items to close the gaps in your core Physical Security policies and processes.

#### Recommended Actions



**1**

**Document the Process:** Formalize and document this policy or process, then ensure accountability to achieve consistency.



**2**

**Ensure enforcement:** Ensure accountability and enforcement to achieve consistency in this policy or process.



**3**

**Conduct Reviews:** Conduct periodic reviews to ensure this policy or process is meeting organizational needs and has been optimized.



**4**

**Maintain solid practices:** Best practices are in place for this policy or process. Maintain optimal status through periodic reviews and continued enforcement.

### How to Optimize

Use the following checklist to ensure that all your Physical Security policies and processes are formalized, documented, enforced, and reviewed.

#### Policies and Processes

#### Optimized

Visitor/guest registration and access policies



Before/after hours access policies



Incorporate physical security considerations into other processes



Audit physical security practices to ensure they are being followed



Perform physical penetration testing



Visible badging policy



Key management and/or card access management practices



### Accountability

Establishing who is accountable for each policy and process is important for enforcement and quality control.

Visitor/guest registration and access policies

Bob Datacrunch

Before/after hours access policies

Joe Computerguy

Incorporate physical security considerations into other processes

Bob Datacrunch

Audit physical security practices to ensure they are being followed

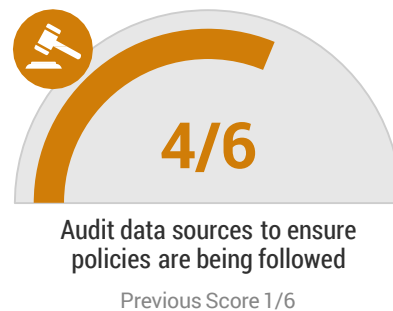
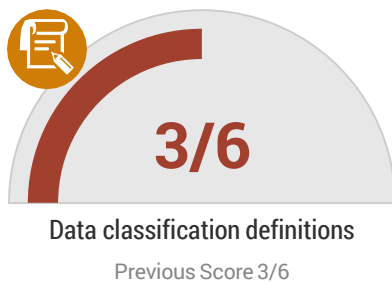
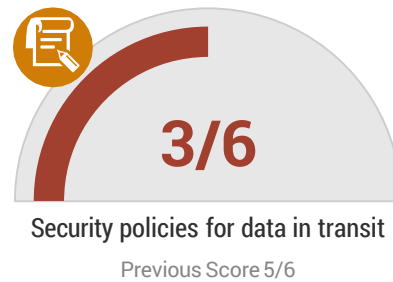
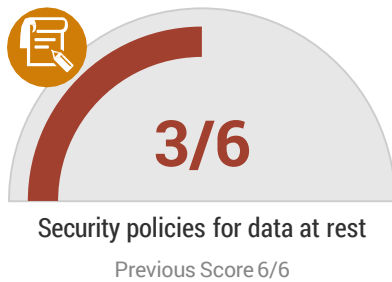
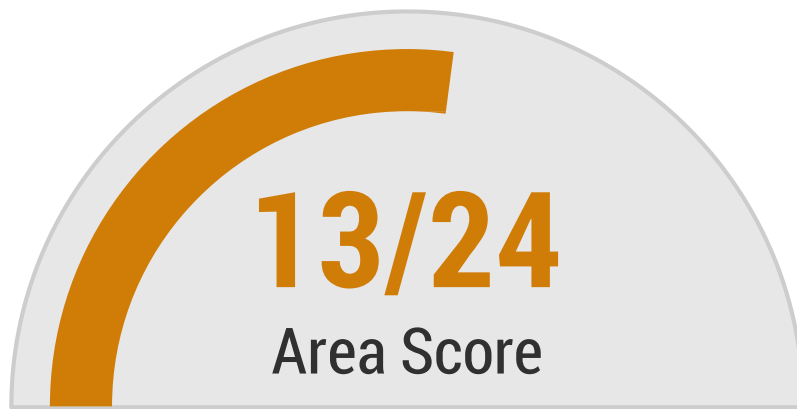
No one - Assign Accountability



Data, or information, is ultimately what it's all about protecting. Ensure that these critical assets are protected against breaches of confidentiality, availability, and integrity.

## Current Scores





"To what extent are the following policies and processes in place for Data Security?"



### How to Improve

Use these action items to close the gaps in your core Data Security policies and processes.

#### Recommended Actions

-  **1 Document the Process:** Formalize and document this policy or process, then ensure accountability to achieve consistency.
-  **2 Ensure enforcement:** Ensure accountability and enforcement to achieve consistency in this policy or process.
-  **3 Conduct Reviews:** Conduct periodic reviews to ensure this policy or process is meeting organizational needs and has been optimized.
-  **4 Maintain solid practices:** Best practices are in place for this policy or process. Maintain optimal status through periodic reviews and continued enforcement.

### How to Optimize

Use the following checklist to ensure that all your Data Security policies and processes are formalized, documented, enforced, and reviewed.

Policies and Processes	Optimized
Security policies for data at rest	<input type="checkbox"/>
Security policies for data in transit	<input type="checkbox"/>
Data classification definitions	<input type="checkbox"/>
Audit data sources to ensure policies are being followed	<input type="checkbox"/>
Security policies for backup data	<input type="checkbox"/>
Require apps to use secure channels for transferring sensitive data	<input type="checkbox"/>
Require offsite backup vendors to meet your security policies for data	<input type="checkbox"/>

### Accountability

Establishing who is accountable for each policy and process is important for enforcement and quality control.

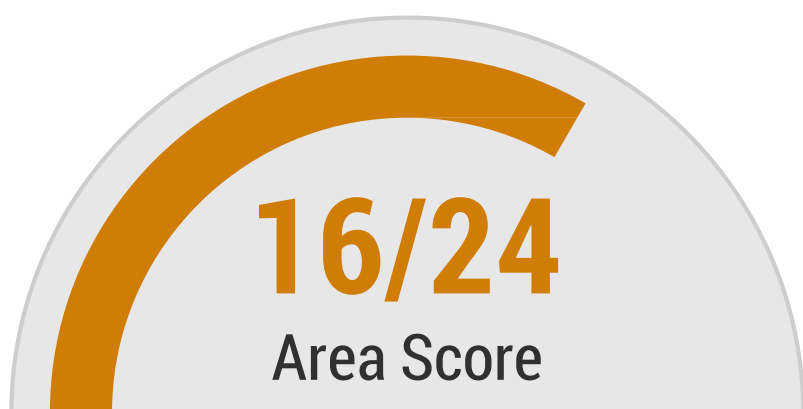
Security policies for data at rest	Bob Datacrunch
Security policies for data in transit	Bob Datacrunch
Data classification definitions	Bob Datacrunch
Audit data sources to ensure policies are being followed	Bob Datacrunch



Server hosts represent the most concentrated stores of valuable information; host security controls protect against wholesale compromise.

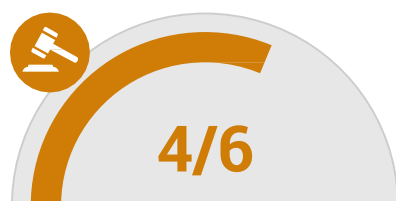
## Current Scores

"To what extent are the following policies and processes in place for Host Security for Servers?"



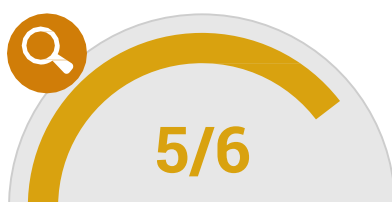
Perform a risk analysis prior to deploying patches/updates

Previous Score 6/6



Internal security standards are defined for each platform

Previous Score 6/6



Complete security checklist as part of deployment and decommissioning

Previous Score 6/6



Audit deployed servers to ensure they still meet security requirements

Previous Score 6/6

### How to Improve

Use these action items to close the gaps in your core Host Security for Servers policies and processes.

#### Recommended Actions

- 1 Document the Process:** Formalize and document this policy or process, then ensure accountability to achieve consistency.
- 2 Ensure enforcement:** Ensure accountability and enforcement to achieve consistency in this policy or process.
- 3 Conduct Reviews:** Conduct periodic reviews to ensure this policy or process is meeting organizational needs and has been optimized.
- 4 Maintain solid practices:** Best practices are in place for this policy or process. Maintain optimal status through periodic reviews and continued enforcement.

### How to Optimize

Use the following checklist to ensure that all your Host Security for Servers policies and processes are formalized, documented, enforced, and reviewed.

Policies and Processes	Optimized
Perform a risk analysis prior to deploying patches/updates	<input type="checkbox"/>
Internal security standards are defined for each platform	<input type="checkbox"/>
Complete security checklist as part of deployment and decommissioning	<input type="checkbox"/>
Audit deployed servers to ensure they still meet security requirements	<input type="checkbox"/>
Audit server deployment practices to ensure policies are being followed	<input type="checkbox"/>

### Accountability

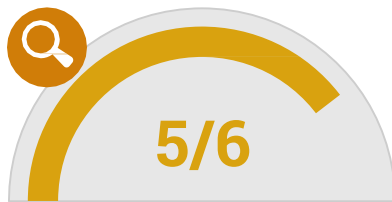
Establishing who is accountable for each policy and process is important for enforcement and quality control.

Perform a risk analysis prior to deploying patches/updates	Jane Techpro
Internal security standards are defined for each platform	Joe Computerguy
Complete security checklist as part of deployment and decommissioning	Joe Computerguy
Audit deployed servers to ensure they still meet security requirements	Joe Computerguy

Managing your users' IDs, and what the users have access to, is a critical factor in reducing the risk of intentional or unintentional data compromise.

## Current Scores

"To what extent are the following policies and processes in place for IAM Security?"



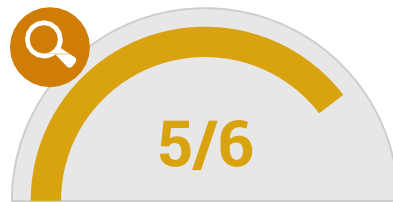
Acceptable use policies for IT services  
Previous Score 5/6



User access levels defined  
Previous Score 5/6



Require management signoff for changes to user access rights  
Previous Score 5/6



Audit user accounts to ensure they still meet requirements  
Previous Score 5/6

### How to Improve

Use these action items to close the gaps in your core IAM Security policies and processes.

#### Recommended Actions

- 1 Document the Process:** Formalize and document this policy or process, then ensure accountability to achieve consistency.
- 2 Ensure enforcement:** Ensure accountability and enforcement to achieve consistency in this policy or process.
- 3 Conduct Reviews:** Conduct periodic reviews to ensure this policy or process is meeting organizational needs and has been optimized.
- 4 Maintain solid practices:** Best practices are in place for this policy or process. Maintain optimal status through periodic reviews and continued enforcement.

### How to Optimize

Use the following checklist to ensure that all your IAM Security policies and processes are formalized, documented, enforced, and reviewed.

Policies and Processes	Optimized
Acceptable use policies for IT services	<input type="checkbox"/>
User access levels defined	<input type="checkbox"/>
Require management signoff for changes to user access rights	<input type="checkbox"/>
Audit user accounts to ensure they still meet requirements	<input type="checkbox"/>
Separation of duties policy	<input type="checkbox"/>
New user deployment policy	<input type="checkbox"/>
Employee termination security policy	<input type="checkbox"/>
Password complexity requirements	<input type="checkbox"/>
Multi-factor identification required	<input type="checkbox"/>
Federated identity management required	<input type="checkbox"/>
Smart card identity management required	<input type="checkbox"/>
User access rights approval policy	<input type="checkbox"/>
Audit IAM practices to ensure policies are being followed	<input type="checkbox"/>

### Accountability

Establishing who is accountable for each policy and process is important for enforcement and quality control.

Acceptable use policies for IT services	Jane Techpro
User access levels defined	Jane Techpro
Require management signoff for changes to user access rights	Jane Techpro
Audit user accounts to ensure they still meet requirements	Jane Techpro

Network security controls protect against external threats, and provide a brake against and potential visibility into threats that originate inside the network perimeter.

## Current Scores

"To what extent are the following policies and processes in place for Network Security?"



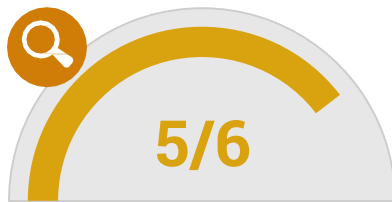
Inbound and outbound traffic control must include IP filtering/traffic-based access control

Previous Score 5/6



Complete a security checklist as part of deployment and decommissioning processes

Previous Score 3/6



Audit deployed networks to ensure they still meet requirements

Previous Score 3/6



Network segmentation policy

Previous Score 5/6

### How to Improve

Use these action items to close the gaps in your core Network Security policies and processes.

#### Recommended Actions

- 1 Document the Process:** Formalize and document this policy or process, then ensure accountability to achieve consistency.
- 2 Ensure enforcement:** Ensure accountability and enforcement to achieve consistency in this policy or process.
- 3 Conduct Reviews:** Conduct periodic reviews to ensure this policy or process is meeting organizational needs and has been optimized.
- 4 Maintain solid practices:** Best practices are in place for this policy or process. Maintain optimal status through periodic reviews and continued enforcement.

### How to Optimize

Use the following checklist to ensure that all your Network Security policies and processes are formalized, documented, enforced, and reviewed.

Policies and Processes	Optimized
Inbound and outbound traffic control must include IP filtering/traffic-based access control	<input type="checkbox"/>
Complete a security checklist as part of deployment and decommissioning processes	<input type="checkbox"/>
Audit deployed networks to ensure they still meet requirements	<input type="checkbox"/>
Network segmentation policy	<input checked="" type="checkbox"/>
TCP/IP services security policy	<input type="checkbox"/>
Perform a risk analysis prior to deploying patches/updates	<input type="checkbox"/>
Employ honeypots to proactively detect threats and update security practices accordingly	<input type="checkbox"/>
Audit network deployment practices to ensure policies are being followed	<input type="checkbox"/>

### Accountability

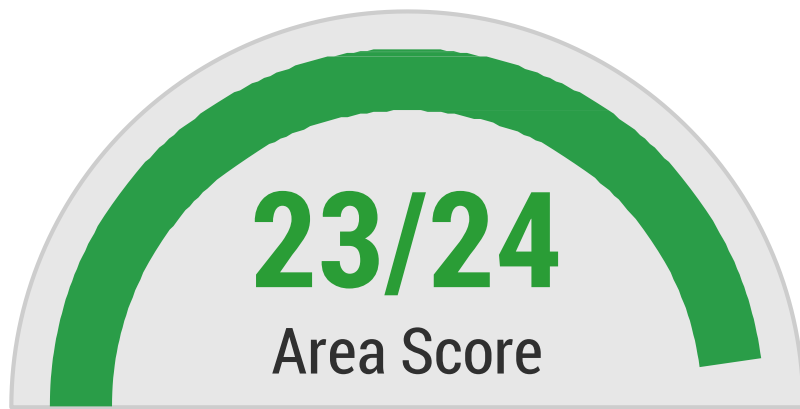
Establishing who is accountable for each policy and process is important for enforcement and quality control.

Inbound and outbound traffic control must include IP filtering/traffic-based access control	Jane Techpro
Complete a security checklist as part of deployment and decommissioning processes	Jane Techpro
Audit deployed networks to ensure they still meet requirements	Joe Computerguy
Network segmentation policy	Jane Techpro

Applications are often the "front door" by which information is accessed; failure to adequately secure apps can result in large scale information breaches.

## Current Scores

"To what extent are the following policies and processes in place for Application Security?"



Require security testing prior to deployment for custom and COTS apps

Previous Score 1/6



Application development projects must include countermeasures to STRIDE

Previous Score 5/6



Network and production data segmentation between Dev/Testing and Production environments

Previous Score 5/6



Audit deployed apps to ensure they still meet security requirements

Previous Score 1/6

### How to Improve

Use these action items to close the gaps in your core Application Security policies and processes.

#### Recommended Actions

- 1 Document the Process:** Formalize and document this policy or process, then ensure accountability to achieve consistency.
- 2 Ensure enforcement:** Ensure accountability and enforcement to achieve consistency in this policy or process.
- 3 Conduct Reviews:** Conduct periodic reviews to ensure this policy or process is meeting organizational needs and has been optimized.
- 4 Maintain solid practices:** Best practices are in place for this policy or process. Maintain optimal status through periodic reviews and continued enforcement.

### How to Optimize

Use the following checklist to ensure that all your Application Security policies and processes are formalized, documented, enforced, and reviewed.

Policies and Processes	Optimized
Require security testing prior to deployment for custom and COTS apps	<input type="checkbox"/>
Application development projects must include countermeasures to STRIDE	<input checked="" type="checkbox"/>
Network and production data segmentation between Dev/Testing and Production environments	<input checked="" type="checkbox"/>
Audit deployed apps to ensure they still meet security requirements	<input checked="" type="checkbox"/>
Application development design documents include internal and external compliance requirements such as legal, regulatory, data confidentiality, security, development, software architecture, and infrastructure	<input type="checkbox"/>
Approved code sources	<input type="checkbox"/>
Require security testing as part of change control procedures for custom and COTs apps	<input type="checkbox"/>
Conduct vulnerability assessments as part of QA prior to deployment	<input type="checkbox"/>
Perform a risk analysis prior to deploying software patches	<input type="checkbox"/>
Audit application development practices to ensure policies are being followed	<input type="checkbox"/>

### Accountability

Establishing who is accountable for each policy and process is important for enforcement and quality control.

Require security testing prior to deployment for custom and COTS apps	Jane Techpro
Application development projects must include countermeasures to STRIDE	Jane Techpro
Network and production data segmentation between Dev/Testing and Production environments	Jane Techpro
Audit deployed apps to ensure they still meet security requirements	Bob Datacrunch