Mikrotik RouterOS Security Audit Checklist

Akbar Azwir / Mikrotik User Meeting Indonesia 2014

belajar MikroTik
www.belajarmikrotik.com

TÜVRheinland®

About me

http://id.linkedin.com/in/akbarazwir/

Akbar Azwir

- Graduated from Binus University
- Certified Trainer since 2008

- Founded Forum Mikrotik Indonesia in 2007
- Working in PT Bayan Resouces Tbk since 2008

- Trainer at BelajarMikrotik.Com

belajar MikroTik
www.belajarmikrotik.com

About me

belajar MikroTik
www.belajarmikrotik.com

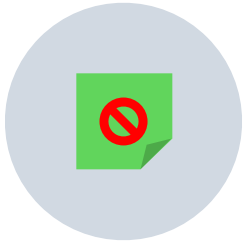
Belajar Mikrotik

- Started in 2013 by Herry Darmawan and Akbar Azwir
- We deliver all Certified Mikrotik class, Academy class, and Integration class
- Working with more than 10 partners we have delivered almost 30 trainings throughout 2014
- Please visit our website at www.belajarmikrotik.com or www.belajarmikrotik.co.id for more information
- Please ask us for training discount coupon during MUM Indonesia 2014 only

Information Security

Information

Assets that has a value which therefor needs protection



Information Security

Preservation of Confidentiality, Integrity, and Availability of an information

Information Security

belajar MikroTik
www.belajarmikrotik.com

Graphic: http://www.cyberintelligence.my/our-approach/

Information Security

There’s no such thing as 100% secure

Information Security is a continuous effort

belajar MikroTik
www.belajarmikrotik.com

Graphic : http://www.iphonefaq.org/archives/ios-501, http://idealway.tumblr.com/post/1434031686/3-reasons-why-continuous-improvement-efforts-fail

ISO/IEC 27001:2013

Information technology – Security techniques – Information security management systems - Requirements

Standards that provides methodology for the implementation of ***Information Security Management System*** in an organization.

Can be implemented in any kind of organization, profit or non-profit, private or state-owned, small or large.

ISO 27001

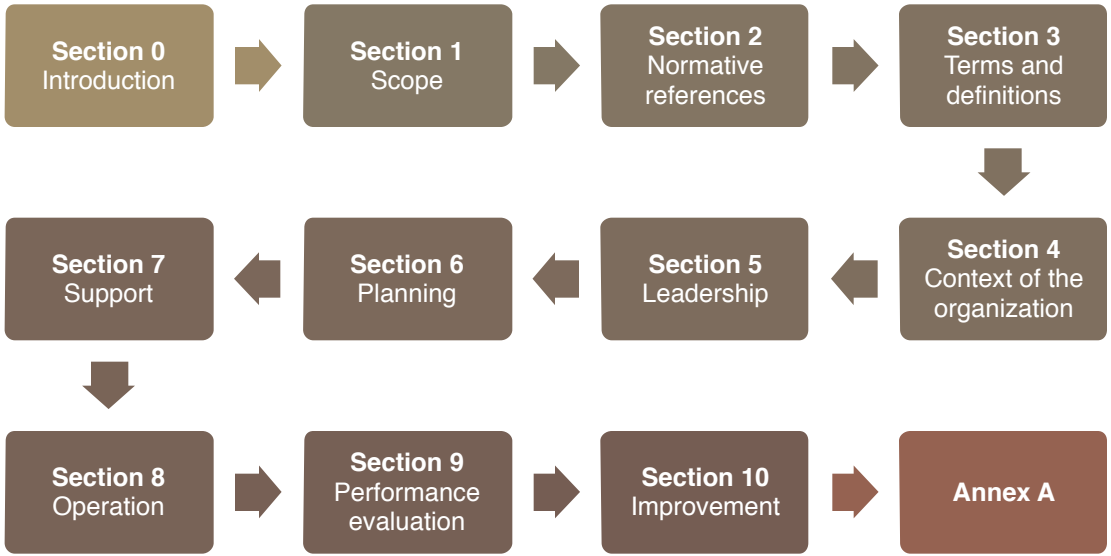
Benefit

- Achieve marketing advantage
- Lower cost
- Better organization
- Comply with legal requirements or regulations

ISO 27001 PDCA Cycle

Graphic : http://www.netgrowthltd.co.uk/ISO27001.aspx

ISO 27001 Structures



Sections 0 to 3 are introductory and are not mandatory for implementation

Sections 4 to 10 contains requirements that must be implemented in an organization if it wants to comply

Annex A contains 114 controls that must be implemented if applicable

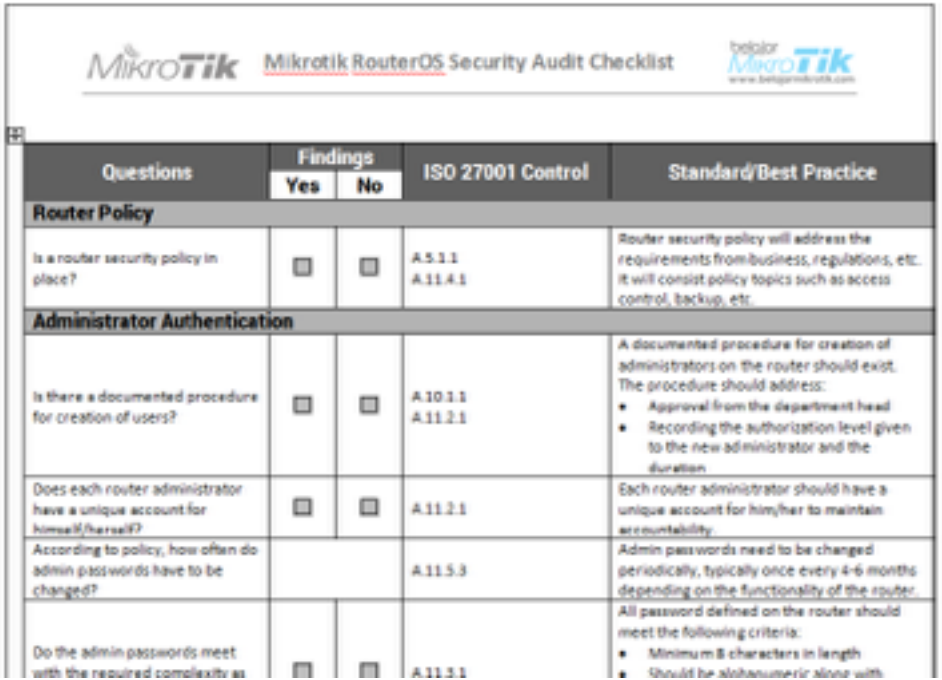
Checklist

Mikrotik RouterOS Security Audit Checklist contains questions based on Annex A controls that are applicable to Mikrotik RouterOS

Derivative work from the same document for Cisco Router from www.iso27001security.com

This is not a security advice document

Ver 0.91 – On going works



MikroTik Mikrotik RouterOS Security Audit Checklist belajar MikroTik

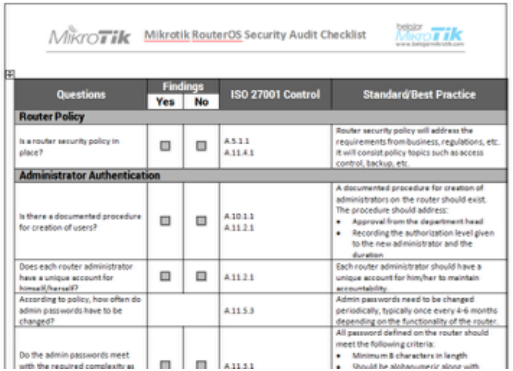
Questions	Findings		ISO 27001 Control	Standard/Best Practice
	Yes	No		
Router Policy				
Is a router security policy in place?	☐	☐	A.5.1.1 A.11.4.1	Router security policy will address the requirements from business, regulations, etc. It will consist policy topics such as access control, backup, etc.
Administrator Authentication				
Is there a documented procedure for creation of users?	☐	☐	A.10.1.1 A.11.2.1	A documented procedure for creation of administrators on the router should exist. The procedure should address: • Approval from the department head • Recording the authorization level given to the new administrator and the duration
Does each router administrator have a unique account for himself/herself?	☐	☐	A.11.2.1	Each router administrator should have a unique account for him/her to maintain accountability
According to policy, how often do admin passwords have to be changed?			A.11.5.3	Admin passwords need to be changed periodically, typically once every 4-6 months depending on the functionality of the router
Do the admin passwords meet with the required complexity as	☐	☐	A.11.3.1	All password defined on the router should meet the following criteria: • Minimum 8 characters in length • Should be alphanumeric along with

Checklist Download

Mikrotik RouterOS Security Audit Checklist is licensed under Creative Commons

Can be downloaded from :

http://www.belajarmikrotik.com/?p=21598



MikroTik Mikrotik RouterOS Security Audit Checklist belajar MikroTik

Questions	Findings Yes	Findings No	ISO 27001 Control	Standard/Best Practice
Router Policy				
Is a router security policy in place?	☐	☐	A.5.1.1 A.11.4.1	Router security policy will address the requirements from business, regulations, etc. It will consist policy topics such as access control, backup, etc.
Administrator Authentication				
Is there a documented procedure for creation of users?	☐	☐	A.10.1.1 A.11.2.1	A documented procedure for creation of administrators on the router should exist. The procedure should address: • Approval from the department head • Recording the authorization level given to the new administrator and the duration
Does each router administrator have a unique account for himself/herself?	☐	☐	A.11.2.1	Each router administrator should have a unique account for him/her to maintain accountability.
According to policy, how often do admin passwords have to be changed?			A.11.5.3	Admin passwords need to be changed periodically, typically once every 4-6 months depending on the functionality of the router.
Do the admin passwords meet with the required complexity as	☐	☐	A.11.5.1	All password defined on the router should meet the following criteria: • Minimum 8 characters in length • Should be alphanumeric along with

Checklist Categories

Router Policy

Contains question regarding the existence of Router Security Policy

Administrator Authentication

Questions about the procedure and technical control on how administrator access to the router

Router Access Management

Questions about services to access routers and snmp usage

Checklist Categories

Configuration Management

Contains question regarding the management of router configuration

Business Continuity

Questions about the procedure for disaster recovery and business continuity

Log Management and Incident Handling

Questions about how the logs are being managed and the procedure for handling any incident

belajar MikroTik
www.belajarmikrotik.com

Thank you

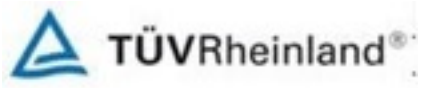
For more info please contact us

akbar@belajarmikrotik.com
www.belajarmikrotik.com

belajar MikroTik
www.belajarmikrotik.com

Credits

Thank you for the support for this presentation



Dirga Yosafat Hyasintus

Sigit Pratomo

Gajendran Kandasamy, PhD

Herry Darmawan

Adhie Lesmana