online business systems

May 11 2021

WHEN YOU DON'T HAVE A CISO

Building a Strong Security Program

Adam Kehler
Director, RSP Healthcare Services

Results. Guaranteed.

online business systems

CAN YOU RELATE?

GETTING STARTED POLL

online business systems

ADAM KEHLER

Director of RSP Healthcare Services
Online Business Systems

Results. Guaranteed.

About Online

Founded in 1986
Privately held for 35 years

Over 350 professionals in Canada & USA

North American Clients Consulting worldwide

"We know that when great people, who share a set of common values, work together, they can accomplish great things."

– Chuck Loewen
President and Chief Executive Officer

Digital Transformation

- Digital Business Transformation
- Customer Experience
- Digital Product Development
- Service Management

Cybersecurity

- Technical Security Services
- Advisory Services
- Assessment Services
- Managed Security Services

"I have forty-eight information technology vendors and just one partner, and that is Online."

– James Nick
Director, PMO

15 consecutive years on Best Workplaces

67 Net Promoter Score against an Industry average of 41

4.7 Company Rating on Glassdoor

99% CEO Approval rating on Glassdoor

AGENDA

01 Trends

02 When You Don’t Have a CISO…

03 What a vCISO can do for you

04 Q &A

online business systems

TRENDS

online business systems

TRENDS WE ARE SEEING

SHARING of INFO

Explosion of consumer Apps that share information

THIRD-PARTIES

Increasing reliance on third parties including cloud platforms

PHISHING

Phishing attacks becoming increasingly targeted and sophisticated

RANSOMWARE

Ransomware continues with added threat of the sale of compromised data

VENDOR MGMT

Security focus in contracts and vendor management programs

online business systems

WHEN YOU DON'T HAVE A vCISO

—

online business systems

YOUR SECURITY OFFICER

does not have information security experience

BUSINESS RESOURCE

Compliance Based

Some Security Training

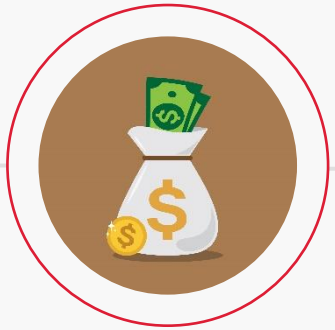
Off the side of the desk

IT LEADER

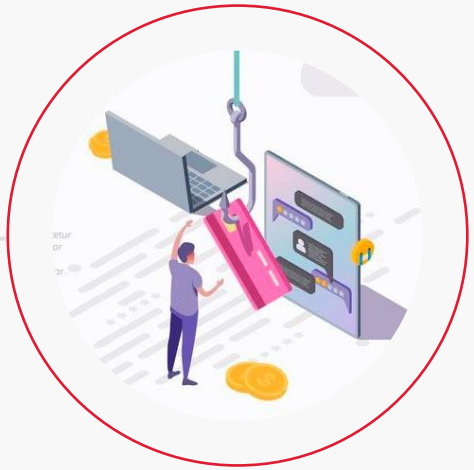
Sounds Technical

Limited understanding of business risk

Off the side of the desk



RANSOMWARE



BREACHES

THE BOARD IS PAYING ATTENTION

Protecting the brand and organizational reputation is critical

The organization needs the ability to translate security risk into business terms

online business systems

YOU JUST HAD A SECURITY RISK ASSESSMENT OR AUDIT

Now What?

RISK ASSESSMENT

RISK MANAGEMENT PLAN

Determine "reasonable and appropriate" security controls.
Put in terms the board will understand.

PROCESSES & TECHNOLOGY

Strategically aligned to your Risk Management Plan

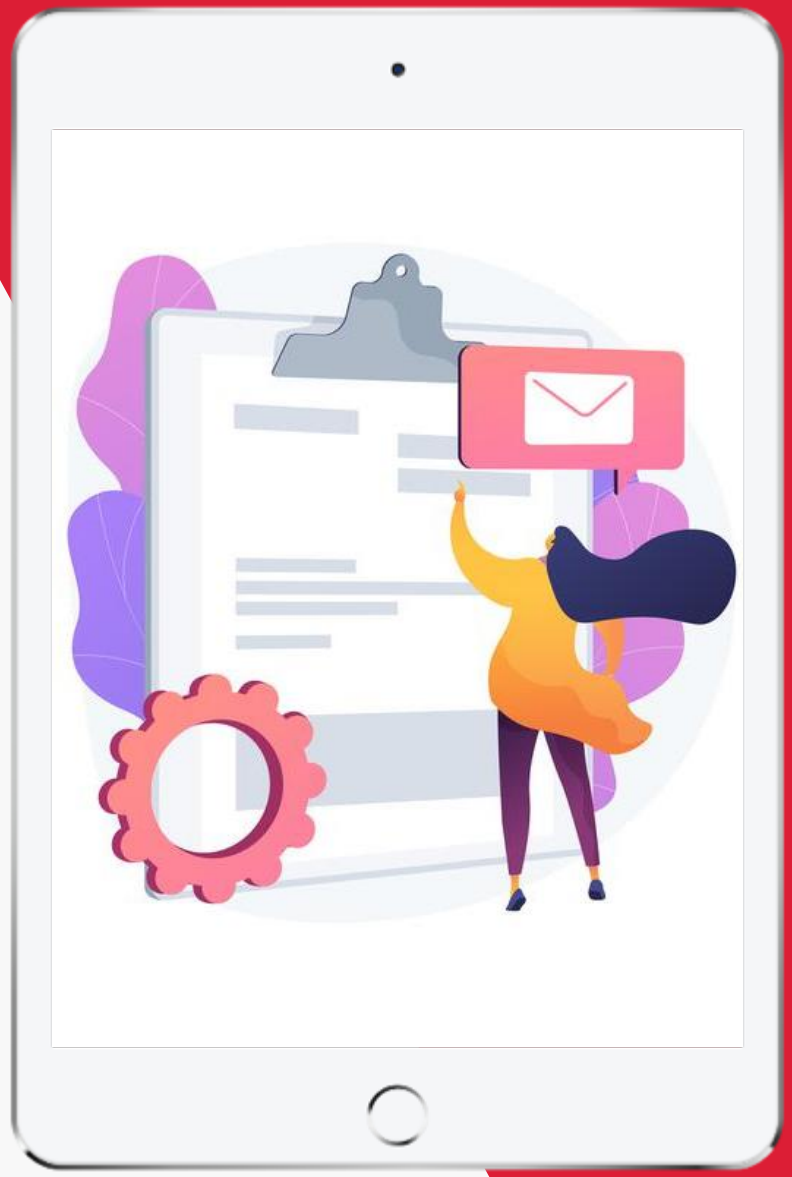
Results. Guaranteed.

online business systems

YOU HAVE COMPLIANCE REQUIREMENTS

FIPPA
PHIA
PIPEDA
PCI-DSS
HITRUST
SOC2

ISO 27001
CCPA
HIPAA



online business systems

YOU HAD A BREACH

It’s not “if” but “when”

Breaches will happen and you need to be prepared. How you respond is critical to mitigating the effects. Coordination of breach response requires working with each part of the business.

It’s not just a technical task.

online business systems

YOU FAILED AN AUDIT

Whether it was a prospective client assessing your security, a certification, or a regulatory audit.

This requires expertise.

online business systems

THE ROLE OF A CISO

online business systems

WHAT A vCISO CAN DO FOR YOU

TAKING A DIFFERENT APPROACH:

A STORY

online business systems

3 PHASES OF A vCISO ENGAGEMENT

PHASE 1

Scope and Baseline

PHASE 2

Assess, Document, Organize

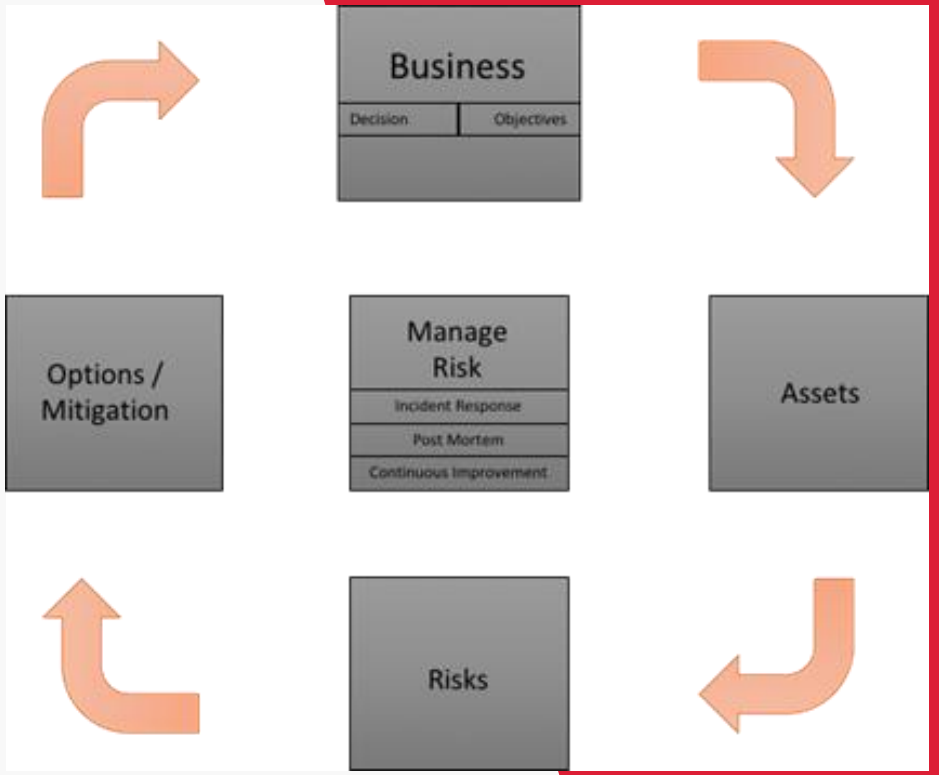
PHASE 3

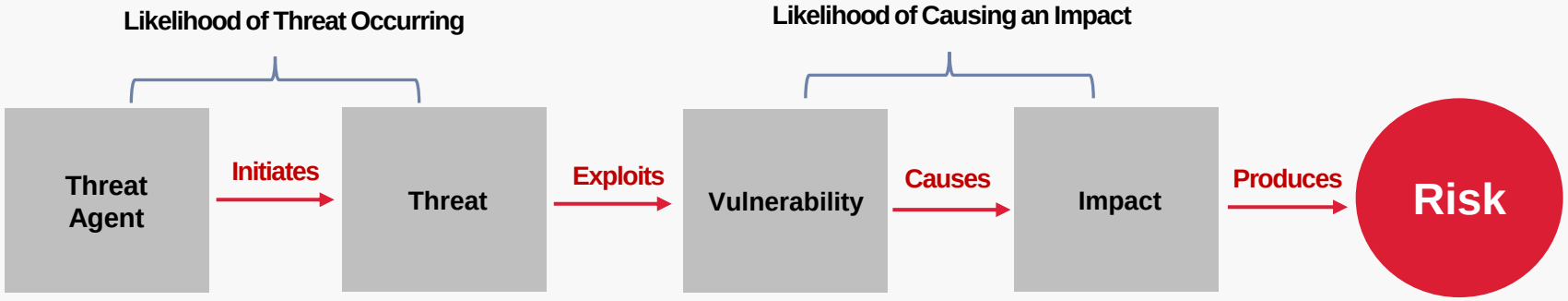
Remediation and Program Management

online business systems

ITRM PROCESS

Enterprise Security Risk Management (ITRM) is a cyclical, iterative approach to managing IT security risk across an enterprise using well-established risk-management principles.

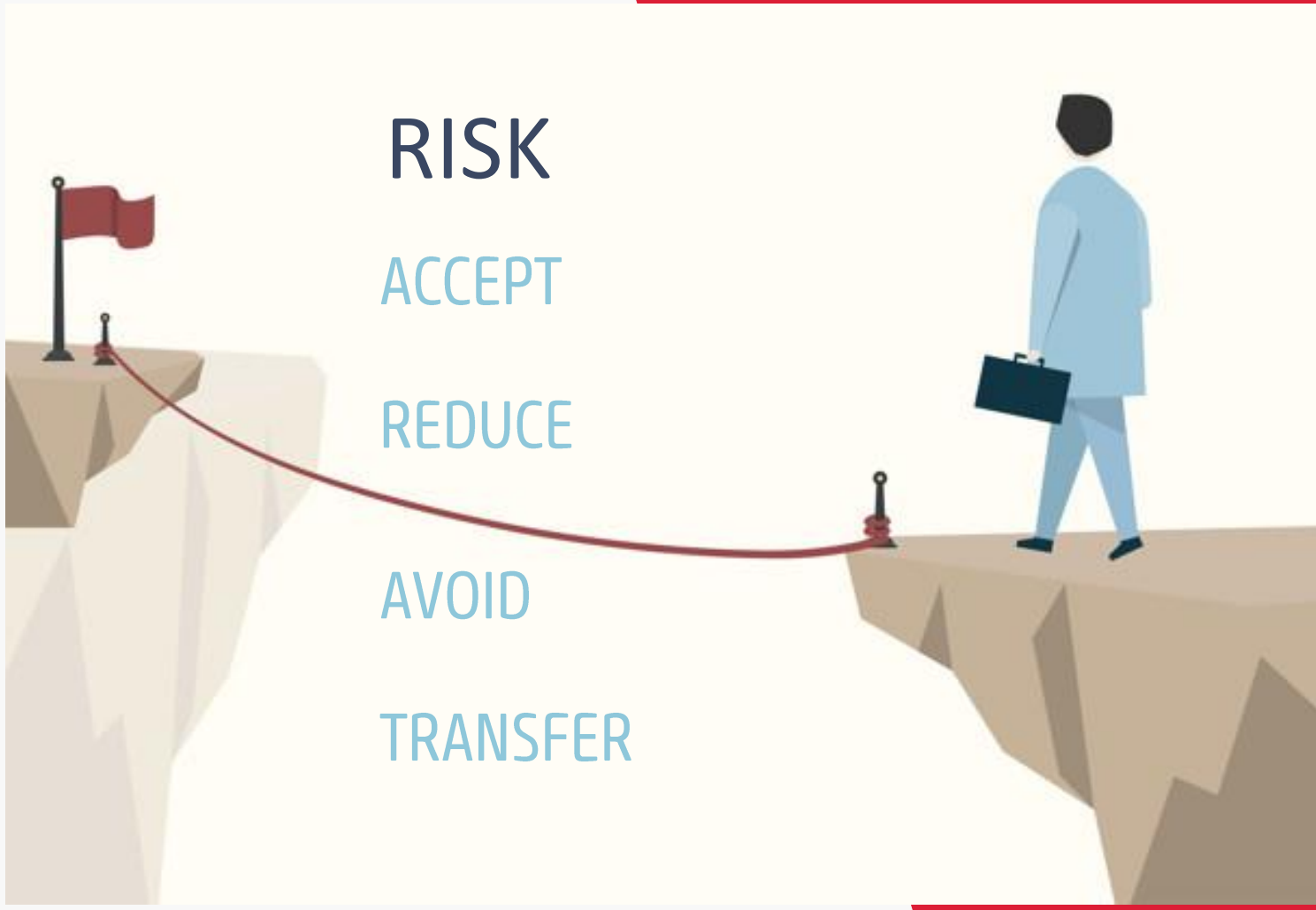




RISK DESCISIONS

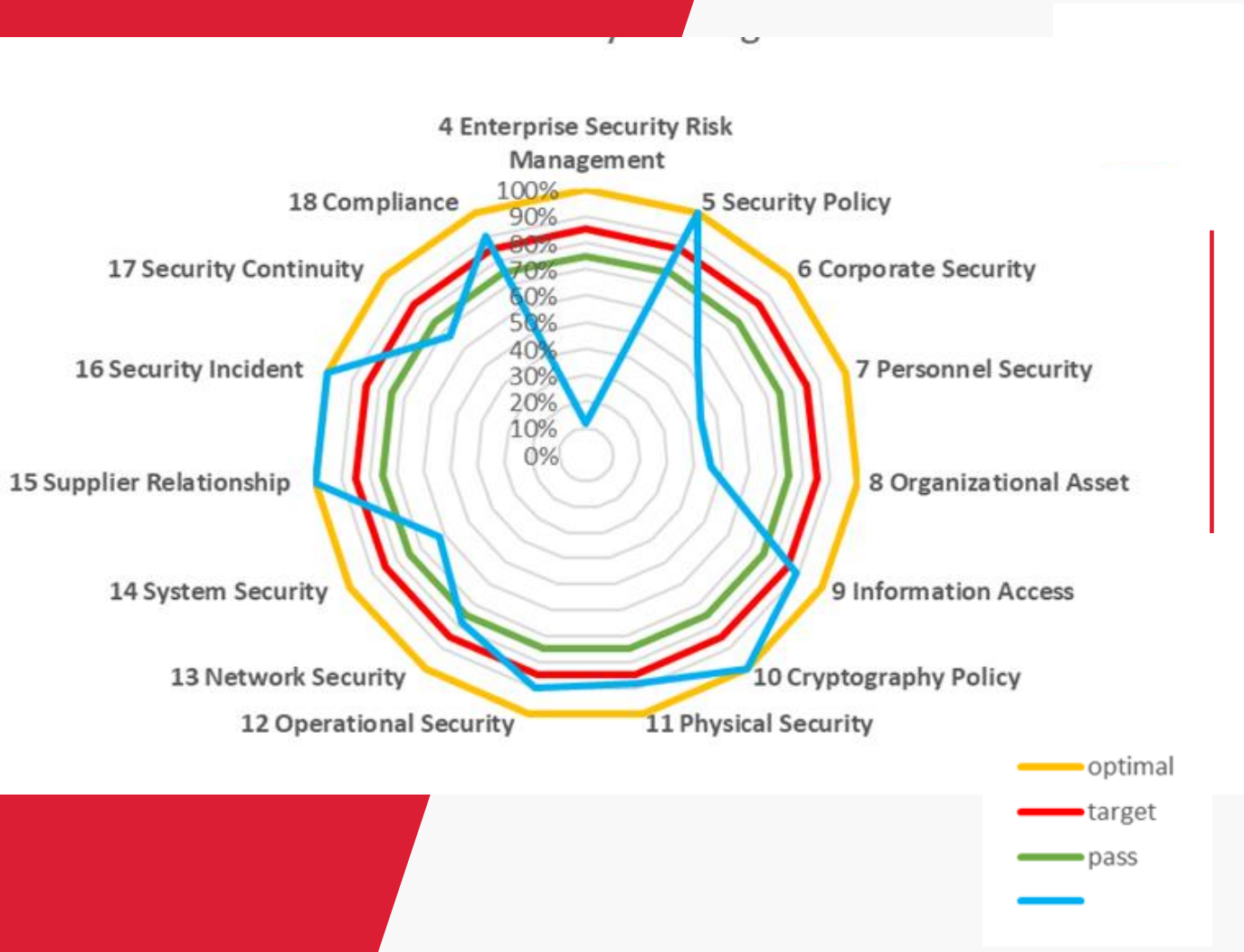
Risk Decisions are determined by the Asset Owner –

not by IT or Cybersecurity



online business systems

SECURITY CONTROLS ASSESSMENT RESULTS



#	Domain	Score
5	Security Policy	100%
6	Corporate Security	55%
7	Personnel Security	44%
8	Organizational Asset	46%
9	Information Access	89%
10	Cryptography Policy	100%
11	Physical Security	88%
12	Operational Security	90%
13	Network Security	78%
14	System Security	62%
15	Supplier Relationship	100%
16	Security Incident	100%
17	Security Continuity	67%
18	Compliance	90%

ISO International Organization for Standardization

SECURITY CONTROLS ASSESSMENT RESULTS

Overall XYZ Company (XYZ) has good security posture with 47% of its security controls and processes already in compliance.

However, with such a high number of security controls that are Non-existent or Initial; and another 33% that require improvement (Managed & Defined), XYZ Company should consider performing a more comprehensive security controls review and associated remediation activities.

Remediation / Implementation ROADMAP

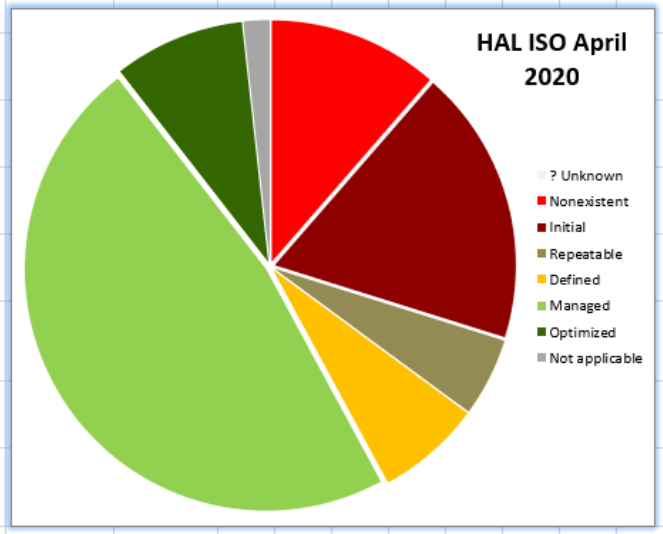
Status of information security controls

Section	Information security control	April 2020 Status	Gaps, Remediation Status, Items & Notes	ISO 27002 Compliance Rating Percentage	Assessment Score
A5	Information security policies				
A5.1	Management direction for information security				
A5.1.1	Policies for information security	Managed			
A5.1.2	Review of the policies for information security	Managed			
A6	Organization of information security				
A6.1	Internal organization				
A6.1.1	Information security roles and responsibilities	Managed			
A6.1.2	Segregation of duties	Initial			
A6.1.3	Contact with authorities	Initial			
A6.1.4	Contact with special interest groups	Managed			
A6.1.5	Information security in project management	Nonexistent			
A6.2	Mobile devices and teleworking				
A6.2.1	Mobile device policy	Defined			
A6.2.2	Teleworking	Defined			
A7	Human resource security				
A7.1	Prior to employment				
A7.1.1	Screening	Nonexistent			
A7.1.2	Terms and conditions of employment	Managed			
A7.2	During employment				
A7.2.1	Management responsibilities	Managed			
A7.2.2	Information security awareness, education and training	Managed			
A7.2.3	Disciplinary process	Managed			
A7.3	Termination and change of employment				
A7.3.1	Termination or change of employment responsibilities	Initial			
A8	Asset management				
A8.1	Responsibility for assets				
A8.1.1	Inventory of assets	Initial			
A8.1.2	Ownership of assets	Nonexistent			
A8.1.3	Acceptable use of assets	Defined			
A8.1.4	Post Employment & Return of assets	Managed			

Introduction | ISMS Requirements | ISO Security Controls | Dashboard | Outstanding Remediation Items

ISO 27002 Remediation Dashboard

Status	Meaning	ISMS States	HAL April ISO 27002 Initial Level of Compliance
? Unknown	Has not even been checked yet	0%	0%
Nonexistent	Complete lack of recognizable policy, procedure, control etc.	0%	11%
Initial	Development has barely started and will require significant work to fulfill the requirements	11%	18%
Repeatable	Progressing nicely but not yet complete	0%	5%
Defined	Development is more or less complete although detail is lacking and/or it is not yet implemented, enforced and actively supported by top management	37%	7%
Managed	Development is complete, the process/control has been implemented and recently started operating	33%	47%
Optimized	The requirement is fully satisfied, is operating fully as expected, is being actively monitored and improved, and there is substantial evidence to prove all that to the auditors	11%	9%
Not applicable	ALL requirements in the main body of ISO/IEC 27001 are mandatory IF your ISMS is to be certified. Otherwise, management can ignore them.	0%	2%



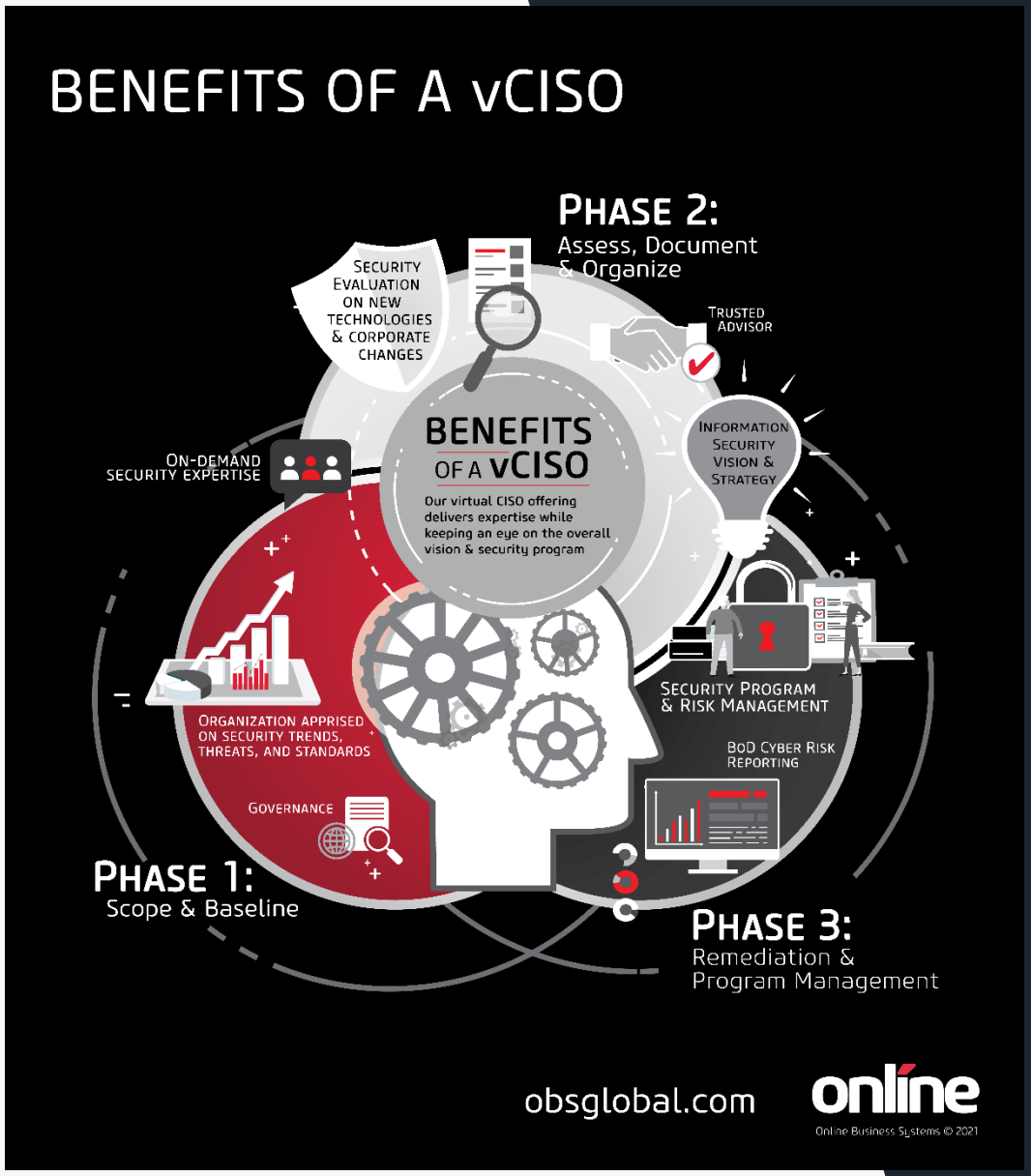
IN CONCLUSION

1. Avoid the pitfalls of assigning information security responsibilities to someone without experience in this area.
2. Hire a CISO that can bridge the gap between the technology and the business
3. A vCISO can be a cost-effective way to achieve these goals

online business systems

OUR BOOTH

- Learn more about vCISO
- Chat with a vCISO
- Access resources



THANK YOU

Enjoy the rest of your day.