YOU

HRV©
Hacker Strategic View

Report V 3.6 –

Index

1. Document History Overview

Document Control Information

Settings	
Document Title:	IT Security - HSV
Project Title:	DRS
Document Authors:	
Doc. Version:	
Sensitivity:	**Confidential**
Date:	

Document Approver(s) and Reviewer(s):

NOTE: All Approvers are required. Records of each approver must be maintained. All Reviewers in the list are considered required unless explicitly listed as Optional.

Name/role	Action	Date
	DRS Draft approval	
	Contributor	
	Reviewer	
	Validator	

Document history:

Changes to this document are summarized in the following table in reverse chronological order (latest version first).

Revision	Date	Created by	Short Description of Changes
V1.00			
V2.00			
V3.01			
V3.01			
V3.02			
V3.03			
V3.04 & 5			
V3.06			

V3.07			

1 a General Introduction

In June 2019, CPE-DRS got the green light to undergo an DRS scan about XXXXX. The prerequisite is what could be found in four hours about XXXXX via a passive external scanning of all publicly available information's, which are of interest from a security point of view. Only information, which highlight security risk or holes, have been taken up.

As a result of that scan, (see Annex 1), CPE-DRS has identified:

- On 3 public IPs 21 malware (now resolved with XXX team).
- A GoDaddy Certificate on https://mail.XXX.be/.
- 23 major security patches on publicly accessible server had not been applied.
- 13 malware identified on https://mail.XX.be/ (now resolved with XXXXX team).
- 2 outdated certificates (now resolved with XXXXX team).
- 30 identified interconnections with XXXXX, but these partners are not monitored and do not have to comply with any security standards of XXXXX. This is one of the easiest ways to enter XXXXX.
- 12 possibilities to bring down XXXXX website and/or all its related services / infrastructure.

On the above base XXXXX has mandated CPE-DRS to undergo a detailed internal scan (see Annex 2) and CPE-DRS has identified 98 concerns.

It is important to highlight that the overall cybersecurity landscape has drastically changed over the past years. Much faster than any IT Infrastructure and Software development departments can potentially adapt to, not to mention the shortening of the time to market companies demands in these fields of supporting activities.

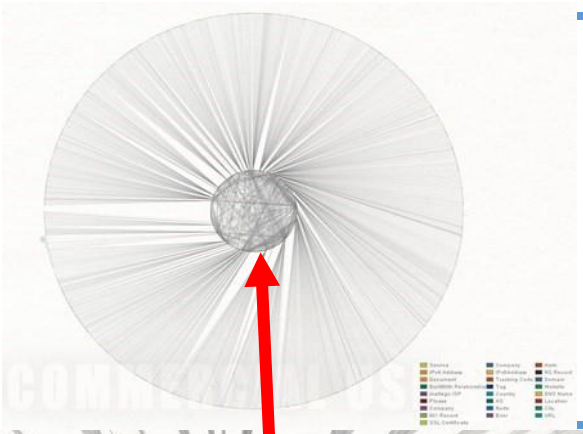
The overall XXXXX global environment is highly complex (see Graph 01) and its dependencies on third parties, may it be on the service side or the connection side has just added an extra layer of risks, that are out of control of XXXXX.

On top the different new legislations (GDPR & NIS) consume budget, technical and human resources, resulting in a lack of time for the high priorities in the day to day activities.

What CPE-DRS has identified is a high commitment of all IT department staff, an incredible flexibility, given the limited overall resources.

As conclusion, yes, there is a great deal of concerns on the cybersecurity side and yes, there are solutions, which will be elaborated in this document.

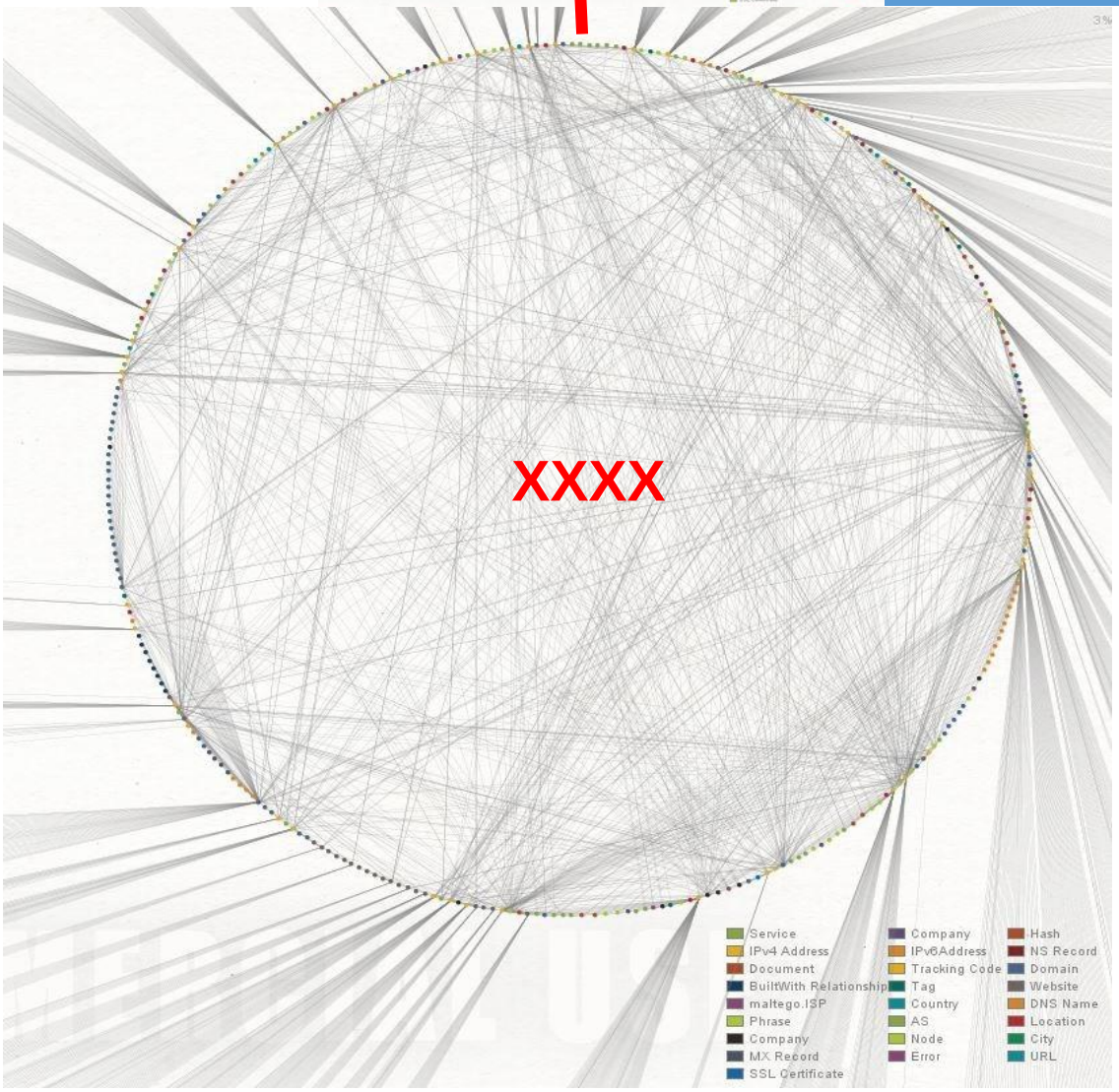
XXXXX and all its interconnectivities & dependencies



View XXXX and the 3rd parties

This represents:

2024 entities
3567 links



Graph 01

1 b Background

Information security is the protection of information from a wide range of threats in order to ensure business continuity and minimise a range of business risks. Essentially, it is the preservation of confidentiality, integrity and availability of information. This is particularly important with the increase in interconnected computing environments and ever-increasing threats.

The present report provides insight into XXXXX' information systems (IS) security. The main objective and scope of this analysis is getting a more alive like picture of the XXXXX's internal and external attack-front. This report has been established in several steps:

- **Step 1: Audit of Security holes & misconfigurations**

  1.a Preparation work by XXXXX
  Installation of ABC appliance

  1.b Installation of 4 passive scanning tools by Christoph Pellkofer
  Installation of 1 appliance – ABC
  Installation of ABCD
  Installation of ABCDE
  Installation of Syslog & compliance Analyser
  Establishing a findings inventory based up on only the ext. scan
  Preparation of remediation plan based up on the ext.

  1.c Analysis of the logs by Christoph Pellkofer
  Completing the findings inventory with the int. scan findings
  Preparation of remediation plan based up on the int. scan
  Establish a Quick fix strategy + needs
  Establish a Mid-term (6months) fix strategy + needs
  Establish a Long-term (36months) fix strategy + needs

  1.d Establish situational *as is* report + presentation

- **Step 2: Quick wins**

  2.a Determine with I.T dept. of XXXXX the implementation roadmap taking into account the identified urgencies in Step 1

  2.b Implementation of the quick win roadmap by Internal IT
  Assistance of C.Pellkofer (Up on demand)

  2.c Weekly check of implementation status & quality
  This 2.b implementation will be done with assistance and support from CPE-DRS .
  CPE-DRS will analyse the implementation on a weekly basis until 31/10/2019.

As our benchmark (BSI-ISO) we used the black hat kill chain for information security. Although this is not a standard, but it reflects the reality in cyber-criminality. It is a good starting point for XXXXX to develop sound information security practices. The implementation of all remediation and the three-track strategy will be based up on ISO 27002. Our findings will diminish considerably the IT security attack fronts.

The security gap analysis provides further insight into how big the gap is between the standards.

1 c What was foreseen to be done

The security gap analysis was conducted across IT Infrastructure. We assessed information security across most security categories defined within ISO 27002. There are essentially 12 areas the standards focus on with each area containing various categories.

The areas are:

- IT internal security concerns
- IT external security concerns
- Information Security Risk Management
- Information Security Incident Management
- Compliance GDPR / NIS
- Operations Management
- Asset Management

Following topics are not in scope of the present assignment.
However, sometimes we discover interesting things that will be gladly commentated.

- Business Continuity Management
- Physical and Environmental Security
- Security Policy
- Human Resources
- Organising Information Security

We assessed whether controls for the categories in each area were effectively being met and if not whether mitigating controls were in place. As part of the assessment against the standards and black hat, we also assessed the following:

- Has XXXXX identified their security requirements by assessing the risks to their business and information systems?
- Has XXXXX selected appropriate controls that mitigate their identified risks, in line with the International Standard?
- Is XXXXX aligned with the International Standard, have other strategies been used to mitigate identified risks?
- What is the degree of alignment with the International Standard across all information systems security categories?

Each area was assessed in terms of its effectiveness in meeting the standards and scored. We rated scores above 85 per cent to be effective, scores between 60 to 85 per cent as partially effective and below 60 per cent as ineffective. Those areas in the standard that were obviously not applicable to XXXXX we audited were not considered.

1 d What was found

Table 1 below represents the results of our gap analysis across XXXXX. XXXXX did not fully meet the requirements of the standards however; anything that has been brought up during the assessment was swiftly resolved, as much as it was possible. It is likely that this result is relevant to XXXXX' management and it demonstrates a lack of good security practices across the company. This puts XXXXX IT systems at high risk.

Area	***XXXXX***
IT internal security concerns	
IT external security concerns	
Information Security Risk Management	
Information Security Incident Management	
Compliance GDPR / NIS	
Operations Management	
Asset Management	
Business Continuity Management	
Physical and Environmental Security	
Security Policy	

Human Resources	
Organising Information Security	

Red = 0%–60% Orange = 61%–85% Green = 86%–100%

Red = ineffective, Orange = partially effective, Green = effective

Analysis

The standards provide guidance on how an organisation should approach information security. The starting point is establishing what the security requirements are and assessing risk. Security requirements can be derived from three main sources which include (1) assessing risks taking into account the overall business strategy and objectives. (2) The legal, statutory and regulatory requirements including. (3) The kill chain.

Our analysis indicated that XXXXX is not taking these first steps by adopting a strategic approach to identifying and assessing risks. This is an important area of initial focus to identify, assess and treat risks and allow XXXXX to take a strategic approach to managing information security. In the absence of a strategic approach, XXXXX lack focus and the approach to security becomes ad hoc. This can lead to XXXXX wasting resources on areas of minimal risk while leaving critical areas exposed.

XXXXX should use their risk assessment to inform the development of business continuity and specific incident management plans. A sound information security policy is important for security governance and should also be informed by the initial risk assessment. A common failing was lack of business continuity management for information security. These plans help to ensure XXXXX can recover or continue to function should a serious incident occur.

XXXXX had not performed in risk assessment that typically demonstrated weaknesses across all areas. Table 1 shows that XXXXX had inadequate controls for at least nine of the 11 areas assessed. This demonstrates a lack of awareness and understanding of the controls required to ensure the security of their environments.

XXXXX has no effective controls in place for Information Security Incident Management or IS Acquisition, Development and Maintenance. XXXXX will not be able to detect and respond to incidents that threaten the security and availability of their environments. Key applications within XXXXX are also more vulnerable to unauthorised access and downtime.

Our analysis suggests XXXXX is focusing on some quick wins such as day to day security incident management and response, as well a 360° ISMS analysis to determine the 36 months global IT strategy.

1 d Security Standards – addressing the gaps

XXXXX can use the standards to perform their own gap analysis and use the results to develop a security improvement plan. This can provide a foundation for setting priorities, assigning ownership, allocating investments of time, money and human resources and for measuring and improving compliance with the standards.

Information security is achieved by implementing suitable controls including policies, procedures, organisational structures and software and hardware functions. These controls need to be implemented, monitored, reviewed and improved where necessary to ensure that specific security and business needs of XXXXX are consistently met.

Depending on XXXXX business objectives and circumstance, all areas of the standard could be equally important. XXXXX needs to take a methodical approach when performing a risk assessment to identify and understand the level of control required for each area. Costs for implementing controls must be balanced against the likely impacts resulting from identified security failures. Risks assessments also need to be re-performed periodically to ensure new risks are captured and managed in a timely manner.

While the International Security Standard is a good starting point, additional controls and guidance may be required depending on XXXXX specific needs and functions. NIS complements XXXXX Security Framework and is a good reference for understanding and implementing good information security practices.

2 General Computer Controls and Capability Assessments

2 a Conclusion

We rune a high-level external scan and an internal scan, as well a general analysis on the overall IT GCC and CA.

From that capability assessments conducted only one of the 12 checking areas did meet our expectations for managing their environments effectively. Two thirds of the checks were not meeting our benchmark expectations.

Management of Changes is in place but is not in a countercheck approach. Physical Security is very light. The Management of IT Risks, IT Security, Operations capacity management need much greater focus.

2 b Background

The objective of our general computer controls (GCC) audit is to determine whether the computer controls effectively support the confidentiality, integrity, and availability of information systems. General computer controls include controls over the information technology (IT) environment, computer operations, access to programs and data, program development and program changes. We focused on the following control categories:

- IT operations
- Management of IT risks
- Information security
- Business continuity
- Change control

We use the results of our GCC work to feed our maturity model. This way we are assessing how well developed and capable the established IT controls are and how well developed or capable they should be. The models provide a benchmark for XXXXX performance and a means for comparing results from year to year.

The models we developed use accepted industry good practice as the basis for assessment. Our assessment of the appropriate maturity level for XXXXX general computer controls is influenced by various factors. These include: the business objectives of XXXXX; the level of dependence on IT; the technological sophistication of their computer systems; and the value of information managed by XXXXX.

2 c What did we do?

We conducted GCC audit and did capability assessment.

We use a 0-5 scale rating[1] listed below to evaluate XXXXX capability and maturity level in each of the GCC audit focus areas. The models provide a baseline for comparing results for XXXXX from year to year. Our intention is to increase the number of agencies assessed each year.

0 (non-existent)	Management processes are not applied at all. Complete lack of any recognisable processes.
1 (initial/ad hoc)	Processes are ad hoc and overall approach to management is disorganised.
2 (repeatable but intuitive)	Processes follow a regular pattern where similar procedures are followed by different people with no formal training or standard procedures. Responsibility is left to the individual and errors are highly likely.
3 (defined)	Processes are documented and communicated. Procedures are standardised, documented and communicated through training. Processes are mandated however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.
4 (managed and measurable)	Management monitors and measures compliance with procedures and takes action where appropriate. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.
5 (optimised)	Good practices are followed and automated. processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the agency quick to adapt.

Table 2 (Rating criteria)

[1] The information within this maturity model assessment is based on the criteria defined within the Control Objectives for Information and related Technology (COBIT 19) manual.

2 d What did we find?

Our capability maturity model assessments show that XXXXX needs to establish better controls to manage their IT operations, IT risks, information security and business continuity. Figure 2 below summarises the results of the capability assessments across XXXXX we audited. We expect XXXXX should be at least within the level three band across all the categories.

Figure 2: Capability Maturity Model Assessment Results

The model shows that the categories with the greatest weakness were Management of IT Risks, Information Security and Business Continuity.

The percentage of XXXXX reaching level three or above for individual categories was as follows:

- IT operations 58 per cent
- Management of IT risks 44 per cent
- IT ext. & int. security 44 per cent
- Business continuity 25 per cent
- Change control 69 per cent
- Asset Management 61 per cent
- Physical security 75 per cent

Area	***Operational Level***	***Security Level***
IT internal security concerns		
IT external security concerns		
Information Security Risk Management		
Information Security Incident Management		
Compliance GDPR / NIS		
Operations Management		
Asset Management		
Business Continuity Management		
Physical and Environmental Security		

Security Policy		
Human Resources		
Organising Information Security		

Red = 0%–60% Orange = 61%–85% Green = 86%–100%
Red = ineffective, Orange = partially effective, Green = effective

2 e IT operations

This is the first year we have assessed IT operations for XXXXX. There has been already an improvement on the remediation of a great deal of the first findings.

Effective management of IT operations is a key element for maintaining data integrity and ensuring that IT infrastructure can resist and recover from security concerns and failures.

We assessed whether XXXXX has adequately defined their requirements for its service levels and allocated resources according to these requirements. We also tested whether service and support levels within XXXXX are adequate and meet good practice.

Some of the tests include whether:

- Policies and plans are implemented and effectively working.
- Repeatable functions are formally defined, standardised, documented and communicated.
- Effective preventative and monitoring controls and processes have been implemented to ensure data integrity and segregation of duties.

Examples of findings:

- XXXXX has incomplete Information Security Policies; nothing is foreseen on the elevated wrights aspect, nor for the end-users or IT staff, which should have specific policies too.
- The overall segregation of duties for users, developers, IT infrastructure administrators,… was found to be ineffective. A sample found employees carrying out incompatible duties.
- At XXXXX, there is no formal service level agreement in place that identifies the agreed service levels provided by their data centre service.

The following section highlights trends over the last five years for the remaining five GCC categories.

2 f Management of IT risks

XXXXX did not meet our expectations for managing IT risks. This area only scored 44 per cent.

Examples of findings:

- XXXXX does not have an end to end risk management process in place for identifying, assessing and treating IT and related risks. Also XXXXX does not have a risk register for ongoing monitoring and mitigation of identified risks in place.
- The method currently used by XXXXX to assess their IT risks was inadequate or ineffective under ISO standards.

XXXXX should have risk management policies and practices that identify, assess and treat risks that affect key business objectives. IT is one of the key risk areas that should be addressed. We therefore recommend XXXXX to have specific risk management policies and practices established such as risk assessments, registers and treatment plans.

Without appropriate IT risk policies and practices, threats may not be identified and treated within reasonable timeframes, thereby increasing the likelihood that XXXXX legal and compliance objectives cannot not be met.

2 g Information security

Today XXXXX scored 44 per cent in the field of IT ext. & int. security, which below our benchmark for effectively managing information security. It is clear from the basic security weaknesses we identified that many areas have not been addressed and implemented. Fundamental security controls to secure their systems and information are not in place, nor a continuous monitoring, resulting in remediation and or endpoint product life cycle management.

Examples of findings:

- XXXXX does not have an effective process in place to ensure that critical software patches and security updates are identified and applied to the network environment and computer systems in a timely manner. Our scans identified a large number of critical and high priority patches which were not applied to databases, operating systems and servers. We also noted that the patching regime was done on an ad hoc basis
- At XXXXX, we found ineffective procedures regarding the monitoring and review of security logs and audit trails within key servers such as the network's Domain Controller and remote access server. XXXXX is not pro-active mode in monitoring of logs to identify unauthorised actions or suspicious activities across the network and servers.
- We reviewed the user access lists for the network's, Active directory and global system and found the following issues:
- 2.158 Domain Administrators have been identified.
- Today XXXXX is not capable to undergo any incident investigation, being proactive about abnormal activities by regrouping endpoints and users, due to an implementation of anonymising users and endpoints.

Information security is critical to maintaining data integrity and reliability of key financial and operational systems from accidental or deliberate threats and vulnerabilities. We examined what controls were established and whether they were administered and configured to appropriately restrict access to programs, data, and other information resources.

2 h Business continuity

To ensure business continuity, XXXXX has in place a business continuity plan (BCP), a disaster recovery plan (DRP), but it does not include an incident response plan (IRP). The BCP defines and prioritises business critical operations and therefore determines the resourcing and focus areas of the DRP. The IRP needs to consider potential incidents and detail the immediate steps to ensure timely, appropriate and effective response.

These plans should be tested on a quarterly basis. Such planning and testing is vital for XXXXX as it provides for the rapid recovery of computer systems in the event of an unplanned disruption affecting business operations and services.

We examined whether plans have been developed and tested. We found that there is no formal IRP in place, that no quarterly testing are undergone, just annually, nor any procedure in place for any evolution of the hardware and software landscape if it has been contaminated by any type of malware, which makes the DRP useless in case of an infection.

2 i Change control

We examined whether changes are appropriately authorised, implemented, recorded and tested. We reviewed any new applications acquired or developed and evaluated the consistency. We also tested whether existing data converted to new systems was complete and accurate.

Examples of findings:

- We found that XXXXX has a formal change management policies in place to ensure all changes to IT systems and applications are handled in a standardised manner, but it is a regular practice to conturn the procedure to accelerate the time to market.
- At XXXXX the current change control procedure does not document important aspects of change management such as:
- The one to one identical implementation between developments – UAT – Production. Deltas exist between all three environments.
- IT security does not validate all codes integrity nor that these can run in production under the IT security standards.
- Need to document, categorise, and test all changes before implementation into the operating environment.

- The processes for classifying and handling non-scheduled (emergency) changes

An overarching change control framework is essential to ensure a uniform standard change control process is followed, achieve better performance, reduced time and staff impacts and increase the reliability of changes. When examining change control, we recommend more detailed procedures are used consistently for changes to it systems and that a delta analysis is undergone on a weekly base to avoid workarounds. The objective of change control is to facilitate appropriate handling of all changes.

There is a risk that without adequate change control procedures, systems will not process information as intended and XXXXX operations and services will be disrupted. There is also a greater chance that information will be lost and access given to unauthorised persons.

2 j Physical security

We examined whether computer systems were protected against environmental hazards and related damage. We also determined whether physical access restrictions are implemented and administered to ensure that only authorised individuals have the ability to access or use computer systems.

We found that XXXXX is not meeting our benchmark.

Examples of findings:

- At XXXXX a number issues with the physical environment were noted.
- XXXXX does not appropriately restrict access to their critical rooms with staff, contractors and maintenance people having unauthorised access.

Inadequate protection of IT systems against various physical and environmental threats increases the potential risk of unauthorised access to systems and information and system failure.

2 k Recommendations

Management of IT operations

- XXXXX should ensure that they have appropriate policies and procedures in place for key areas such as IT risk management, information security, business continuity and change control. IT Strategic plans and objectives support the business strategies and objectives. We recommend the use of standards and frameworks as references to assist XXXXX with implementing good practices.
- XXXXX has limited internal resources and skills, by we recommend to put in place a monitoring and remediation service (SOC).

Management of IT risks

- XXXXX needs to ensure that its risks are identified; assessed and treated within appropriate timeframes and that these practices become a core part of business activities. You should implement a risk register that centralises all IT aspects (Configuration, changes, incidents, financial aspects such as the acquisition costs + staff costs)… to be able to set your risk scores and by so your priorities. This will avoid any personal initiatives based up on personal affinities and hasty actions.

Information security

- XXXXX should ensure good security practices are implemented, up-to-date and regularly tested and enforced for key computer systems. XXXXX must conduct ongoing reviews for user access to systems to ensure they are appropriate at all times.
- The continuous log, configuration and changes must be monitored and registered in a central DB of at least 6 months historical data. This is essential for any time of incident, to be able to debug, go for a reverse or forensic analysis. In case of a breach all legal supporting elements will be at your disposal; e.g. GDPR, stolen hardware / code / data…

Business continuity

- XXXXX should have a business continuity plan, a disaster recovery plan and an incident response plan that is un-existing. DRP backups should be tested in a replicated virtual environment as the likelihood of a downtime is in 80% due to malware (Disposable IT virtual infrastructure). If these are not identified in the DRP a restore has very little sense.
- XXXXX should undergo atleast 4 annual disaster recovery drills per year.
- Ideally XXXXX should implement a full end to end virtual IT infrastructure replication which is a daily disposable environment. This is a must for the DRP but also for a continuous 360° automated + manual pentesting & monitoring of your production + change IT environment.

Change control

- Change control processes should be well developed and consistently followed for changes to computer systems. All changes should be subject to thorough planning and impact assessment

to minimise the likelihood of problems. Change control documentation should be current, and approved changes formally tracked – No more tolerated workarounds.

Physical security

- XXXXX should develop and implement physical and environmental control mechanisms to prevent unauthorised access or accidental damage to computing infrastructure and systems.

General concerns

- XXXXX should re-shift its budget allocation in a more balanced way. Software development is overbudgeted; consequently, the global XXXXX information infrastructure is put at risk.
- Annexe 1 & 2 have been reviewed with the management to set the priorities. These will be categorised in three groups. To realise these remediation objectives it is obvious that the different sections of XXXXX IT department will need a provisional staffing reinforcement. This can only be evaluated once the categorising has been done:

    1. Quick Win / Urgent – as soon as possible, but in less then a month
    2. Important – in a month but less then 3 months
    3. Strategical – 3 months up to 36 months

- Establish a supportive cyber security monitoring partnership, as at XXXXX there are no resources available, nor the skills. CPE-DRS attached to this document a proposal for the service.

3 a EXTERNAL DRS SCAN - Annex 1

Security Issues

CVE-2014-0117 The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.

CVE-2014-0118 The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.

CVE-2016-0736 In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.

CVE-2015-3185 The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2015-3184 mod_authz_svn in Apache Subversion 1.7.x before 1.7.21 and 1.8.x before 1.8.14, when using Apache httpd 2.4.x, does not properly restrict anonymous access, which allows remote anonymous users to read hidden files via the path name.

CVE-2018-1312 In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

CVE20164975 Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

CVE-2016-8612 Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

CVE-2014-0226 Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE- Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache

2014- HTTP Server 2.4.x before 2.4.10 on Windows, when the default AcceptFilter is enabled, allows remote **3523** attackers to cause a denial of service (memory consumption) via crafted requests.

In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured **CVE-** with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset **2017-** encoding when verifying the user's credentials. If the header value is not present in the charset **15710** conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline **CVE-** character in a malicious filename, rather than matching only the end of the filename. This could be **2017-** exploited in environments where uploads of some files are are externally blocked, but only by matching **15715** the trailing portion of the filename.

CVE- The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server **2013-** before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows **6438** remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

CVE- In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end **2017-** of a buffer when sending a malicious Content-Type response header. **7679**

CVE- In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before **2018-** decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions **17199** since the expiry time is loaded when the session is decoded.

mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different **CVE-** arguments within different contexts, which allows remote attackers to bypass intended access **2014-** restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated **8109** by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.

Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This **CVE-** affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an **2017-** unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free **9798** issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

CVE- In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the **2016-** server to crash, and each instance continues to crash even for subsequently valid requests. **2161**

CVE- The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism,

2014- which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script **0231** that does not read from its stdin file descriptor.

The cache_invalidate function in modules/cache/cache_storage.c in the mod_cache module in the **CVE-** Apache HTTP Server 2.4.6, when a caching forward proxy is enabled, allows remote HTTP servers to **2013** cause a denial of service (NULL pointer dereference and daemon crash) via vectors that trigger a missing **4352** hostname value.

CVE- The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server **2014-** before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) **0098** via a crafted cookie that is not properly handled during truncation.

In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI **CVE-** applications (SessionEnv on, not the default), a remote user may influence their content by using a **2018-** "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to **1283** forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted **CVE-** from requests and sent in response lines and headers. Accepting these different behaviors represented **2016-** a security concern when httpd participates in any chain of proxies or interacts with back-end application **8743** servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

3 b Internal Scan - Annex 2

N°	Findings IN 10 DAYS OF INTERNAL SCAN	P&V Project	Projects	SOC combined Solution							Status	Effort Estimation Man/Day	C1	C-2	C3	Type of Resources Int. / Ext. / Mix
1	1559 Windows 10 Domain Admin Laptop / PC / VM	Active Directory	DC	Ad Auditor Plus	Syslog Analyser		Centrify	Verinice	Parrot Sec	P&V SIEM		2	X			Mix 50-50
2	164 Windows 7 Domain Admin Laptop / PC / VM	Active Directory	DC	Ad Auditor Plus	Darktrace	Syslog Analyser	Centrify	Verinice	Parrot Sec	P&V SIEM		2	X			Mix 50-50
3	Revue the overall delegation of controls - In acccordance with the IAM project	Active Directory	DC	Ad Auditor Plus	Darktrace	Syslog Analyser		Verinice	Parrot Sec	P&V SIEM		240			X X X	Mix 50-50
4	Abuse of rights from external consultant; e.g. using service accounts to change GPO, attributes, OU... - In acccordance with the CISO Policy project - THIS IS PART OF THE PAM PROJECT	Active Directory	DC - External AD	Ad Auditor Plus	Darktrace	Syslog Analyser	Centrify	Verinice	Parrot Sec	P&V SIEM		30			X X X	Mix 50-50
5	AD federation with external to XXXXX partners due to Skype	Active Directory	DC - External AD	Ad Auditor Plus	Darktrace	Syslog Analyser		Verinice	Parrot Sec	P&V SIEM		30			X X X	Mix 50-50
6	AD: Users and their AD group 275.387 - Build new Forest / OU / GPO....	Active Directory	DC	Ad Auditor Plus	Darktrace	Syslog Analyser		Verinice	Parrot Sec	P&V SIEM		880			X X X	Mix 50-50
7	Anonymous connection authorised	Active Directory	GPO	Ad Auditor Plus	Darktrace	Syslog Analyser	Centrify	Verinice	Parrot Sec	P&V SIEM		60	X		X X X	Mix 50-50
8	Copying of user profiles should be forbidden : user on and offboarding must be	Active Dire	GPO	Ad Auditor Plus	Darktrace	Syslog Analyser		Verinice	Parrot Sec	P&V SIEM		4	X		X X X	Mix 50-50

	under control with an automation tool	*ctor y*														
9	*Data on the XXXXX SharePoint (OneDrive, Teams, ...) can be directly approached via user + password*	*Acti ve Dire ctor y*	*DC - DT_DLPM - DC - External AD - XXXXX Project MFA*	*Ad Auditor Plus*	*Darktra ce*	*Syslog Analyser*		*Verini ce*	*Parr ot Sec*	*P& V SIE M*		*20*			*X X X*	*Mix 50-50*
10	*DC-trusted federation – No subdomains * Skype*	*Acti ve Dire ctor y*	*DC - External AD*	*Ad Auditor Plus*	*Darktra ce*	*Syslog Analyser*		*Verini ce*	*Parr ot Sec*	*P& V SIE M*		*30*			*X X X*	*Mix 50-50*
11	*GPO are being adapted by IT internal & external staff...*	*Acti ve Dire ctor y*	*DC*	*Ad Auditor Plus*	*Darktra ce*	*Syslog Analyser*		*Verini ce*	*Parr ot Sec*	*P& V SIE M*		*2*	*X*			*Mix 50-50*
12	*GPO inheritance inconsistencies / break*	*Acti ve Dire ctor y*	*DC*	*Ad Auditor Plus*		*Syslog Analyser*		*Verini ce*	*Parr ot Sec*	*P& V SIE M*		*10*		*X X*		*Mix 50-50*
13	*Install AppLocker to block PowerShell*	*Acti ve Dire ctor y*	*GPO - XXXXX requested to scan the network and analyse the logs for none authorised PowerShell*	*Ad Auditor Plus*	*Darktra ce*	*Syslog Analyser*		*Verini ce*	*Parr ot Sec*	*P& V SIE M*		*4*	*X*			*Mix 50-50*
14	*Local-admin passwords are unambiguous and are not be changed, they only use minimum required GPO 8 Hex-Dec*	*Acti ve Dire ctor y*	*GPO - OU*	*Centrify*	*Syslog Analyse r*			*Verini ce*	*Parr ot Sec*	*P& V SIE M*		*2*	*X*			*Mix 50-50*
15	*More secured file server, splitted between environments(non-prod, development, UAT, production)*	*Acti ve Dire ctor y*	*GPO - OU - Network Segmentati on*	*Ad Auditor Plus*	*Darktra ce*	*Syslog Analyser*	*Centrify*	*Verini ce*	*Parr ot Sec*	*P& V SIE M*		*30*			*X X X*	*Mix 50-50*
16	*NO LPO*	*Acti ve Dire ctor y*	*GPO*	*Ad Auditor Plus*	*Darktra ce*	*LanSwee per*	*Syslog Analyser*	*Verini ce*	*Parr ot Sec*	*P& V SIE M*		*60*		*X X*		*Mix 50-50*
17	*No more local admin users on endpoints*	*Acti ve Dire ctor y*	*GPO*	*Ad Auditor Plus*	*Darktra ce*	*LanSwee per*	*Syslog Analyser*	*Verini ce*	*Parr ot Sec*	*P& V SIE M*		*4*	*X*			*Mix 50-50*
18	*No segregation of duties*	*Acti ve Dire ctor y*	*OU - GPO - IAM*	*Ad Auditor Plus*	*Darktra ce*	*Syslog Analyser*	*Centrify*	*Verini ce*	*Parr ot Sec*	*P& V SIE M*		*20*			*X X X*	*Mix 50-50*
19	*Seeing the amount of individual applications, it seems that users rights are either too high or support does install up on demand any application*	*Acti ve Dire ctor y*	*GPO*	*Ad Auditor Plus*	*Darktra ce*	*LanSwee per*	*Syslog Analyser*	*Verini ce*	*Parr ot Sec*	*P& V SIE M*		*20*			*X X X*	*Mix 50-50*
20	*SMB 1 comb. With RDP = perfect exfiltration - To be tested on the API level*	*Acti ve Dire ctor y*	*GPO*	*Ad Auditor Plus*	*Darktra ce*	*LanSwee per*	*Syslog Analyser*	*Verini ce*	*Parr ot Sec*	*P& V SIE M*		*3*	*X*			*Mix 50-50*
21	*Unacceptable Administrators identified 528*	*Acti ve Dire ctor y*	*GPO*	*Ad Auditor Plus*	*Darktra ce*	*LanSwee per*	*Syslog Analyser*	*Verini ce*	*Parr ot Sec*	*P& V SIE M*		*2*	*X*			*Mix 50-50*
22	*Unprotected file sharing with external parties (current projects are not landing at all)*	*Acti ve Dire ctor y*	*DC - External AD*	*Ad Auditor Plus*	*Darktra ce*	*Syslog Analyser*	*Centrify*	*Verini ce*	*Parr ot Sec*	*P& V SIE M*		*15*			*X X X*	*Mix 50-50*
23	Lack of budget and resources for Infrastructure	CIO						Verini ce								
24	Lack of resources on all Infrastructure level to fulfil all the D2D task and at the same time the projects	CIO						Verini ce								

25	Policies & SLA for DC federated partners (systems / networks) with third parties outside the EEA (eg SQS) set up today without any form of control and / or control of mitigating measures such as an addendum to the contract. A procedure comes first to steer everything in the right direction	CISO	Policies / SLA / 3rd Parties Audite					Verinice							X X X	
26	No segregation of duties	CISO	Policy					Verinice						X X		
27	Lack of configuration management between development vs UAT vs production	CISO	Policy					Verinice						X X		
28	Security Awareness	CISO	Training / Supporting material					Verinice						X X	X X X	
29	CISO should report to the CEO and not to the CIO.	CISO						Verinice	Parrot Sec	P&V SIEM			X			
30	DDOS protection on external portals	Cloudflare	Network	Cloudflare	Darktrace			Verinice	Parrot Sec	P&V SIEM		30		X X		Mix 50-50
31	Core switch should ONLY be Cisco : support issues, compatibility issues, knowledge issues	Core Switch	Network	CISCO				Verinice	Parrot Sec	P&V SIEM		20			X X X	Mix 50-50
32	NAC authentication for physical connections	Core Switch	Network	CISCO				Verinice	Parrot Sec	P&V SIEM		15			X X X	Mix 50-50
33	None XXXXX endpoints have access to the network - only to guestLan or with a visitor PC/Laptop	Core Switch	Network	CISCO				Verinice	Parrot Sec	P&V SIEM		2			X X X	
34	97 XXXXX free Dropbox accounts with 410GB of data were reported. This risk urgently needs to be mitigated by a professional solution to provide for the entire organization. - Solution White list	Firewall	Network	Firewall	Darktrace			Verinice	Parrot Sec	P&V SIEM		2	X			Int.
35	Logical access security including the Segregation of Duties is not guaranteed. The IAM program is used as an excuse for not entering it invest during the day to day work.	IAM	IAM / DC / Policy / PAM	Ad Auditor Plus	Darktrace	Syslog Analyser		Verinice	Parrot Sec	P&V SIEM		60			X X X	Mix 50-50
36	Hardcoded in-house developed software – High impact on updating and migration duties	Out of scope							Parrot Sec	P&V SIEM				X X		
37	No coding and development standardisation, nor code revisiting, security checks or validations of compliance for production	Out of scope							Parrot Sec	P&V SIEM				X X		
	environment. Software development has higher priorities as the production / infrastructure - HIGH RISK															
38	No D2D analysis of all security related activities.	Out of scope							Parrot Sec	P&V SIEM				X X		
39	*IoT devices are connected directly to the internal network.*	*Physical Segmentation*	*Network*	*LanSweeper*	*Darktrace*			*Verinice*	*Parrot Sec*	*P&V SIEM*		300			X X X	Mix 50-50
40	*IoT devices FM (lifts, ...) are connected directly to the internal network.*	*Physical Segmentation*	*Network*	*LanSweeper*	*Darktrace*	*Syslog Analyser*		*Verinice*	*Parrot Sec*	*P&V SIEM*						

41	*More secured file server, splitted between environments(non-prod, development, UAT, production)*	*Physical Segmentation*	*XXXXX Project Fileserver Consilidation*	*LanSweeper*	*Darktrace*	*Syslog Analyser*		*Verinice*	*Parrot Sec*	*P&V SIEM*		*300*		*X X*		*Mix 50-50*
42	*No segmentation of IT networks to be set up for NLBt test and build servers. Dev/UAT/Prod*	*Core Switch*	*Network*	*LanSweeper*	*Darktrace*	*Syslog Analyser*		*Verinice*	*Parrot Sec*	*P&V SIEM*		*30*			*X X X*	*Mix 50-50*
43	Physical security (Iot, building mgmt., cameras, badges) managed by different companies implementing unprotected solutions, should also be a physical separate network with new cisco network equipment : complete redraw from the grounds up	Physical Segmentation & CISO	Network + Policies / SLA / 3rd Parties Audite		Darktrace	Centrify		Verinice	Parrot Sec	P&V SIEM		TBA			X X X	
44	Proxy tunnels are used to pass through the XXXXX firewalls.	Physical Segmentation	Network + Systems	Firewall	Darktrace	Syslog Analyser	Security Ognien	Verinice	Parrot Sec	P&V SIEM		10		X X		Mix 50-50
45	*VmWare NSX micro segmentation should be deployed*	*Physical Segmentation*	*High dependency and a must that the Core Switch are replaced by Cisco*	*LanSweeper*	*Darktrace*			*Verinice*	*Parrot Sec*	*P&V SIEM*		*50*		*X X*		*Ext.*
46	*Password management: 1 admin user per clients and 1 admin for servers should be forbidden => PAM solution will maybe help? Easier quick wins could be possible*	*Privliged Access Management*	*Systems + IAM*	*Centrify*	*Ad Auditor Plus*	*Syslog Analyser*		*Verinice*	*Parrot Sec*	*P&V SIEM*		*300*		*X X*		*Mix 50-50*
47	*Remote code execution (Tomcat & Jenkins)*	*Privliged Access Managemente nt*	*Systems + GPO*	*ABC*	*Syslog Analyser*	*Centrify*		*Verinice*	*Parrot Sec*	*P&V SIEM*						
48	Use default passwords for admin accounts.	Privliged Access Management	Systems	ABC	Syslog Analyser	Centrify	Lansweeper	Verinice	Parrot Sec	P&V SIEM		2		X X		Ext.
49	All Servers without AV Software 434 only on ESX level / not local	RESOLVED						Verinice								
50	Expired certificate	RESOLVED						Verinice								
51	The external firewall cannot decrypt all sessions due to used up resources. We do not have a view on the numbers of whether or not flows.	RESOLVED						Verinice								
52	The network configuration with regard to the SAP router is insufficiently secure (strict)	RESOLVED						Verinice								
53	Workstation AV disabled 297 (Windows defender is not a solution)	RESOLVED						Verinice								
54	Workstation AV expired (21)	RESOLVED						Verinice								
55	Workstation without AV 1	RESOLVED						Verinice								
56	Encryption for data in the cloud should be a must	RFP														

57	Centralised management of all Linux servers, this includes also the password management	RFP														
58	Backup Strategy with virtualisation replication solution - Enables continuas Pentest in Non Production	RFP														
59	1.558 W-10 workstations are not up to date on the OS level	Servicing	Patch Management	LanSweeper				Verinice	Parrot Sec	P&V SIEM		6		XX		Int.
60	101 W-2016 servers are not up to date	Servicing	Patch Management	LanSweeper				Verinice	Parrot Sec	P&V SIEM		15		XX		Int.
62	3.085 inventoried license keys. It can be concluded that no or wrong central license management is in place.	Servicing	Asset Management	LanSweeper				Verinice	Parrot Sec	P&V SIEM		15		XX		Mix 50-50
63	5.983 assets have been identified on the network	Servicing	Asset Management	LanSweeper	Darktrace			Verinice				Continius Monitoring and controling - SOC				
64	71.791 installed windows features	Servicing	Asset Management	LanSweeper				Verinice				Continius Monitoring and controling - SOC				
65	Advanced rights can be obtained via a detour -> Windows & Linux patching	Servicing	Patch Management	ABC				Verinice	Parrot Sec	P&V SIEM		20		XX		Mix 50-50
66	1.189 Apps in average per user (Bios/OS/Driver/ Soft……)	Servicing	Baseline image	LanSweeper	Darktrace	Syslog Analyser		Verinice				Continius Monitoring and controling - SOC				
67	external IT with little to no insight from our side, not following any of our policies but using our internet and exchanging more and more data : pseudo shadow IT supported by management	CISO	Policies / SLA / 3rd Parties Audite	LanSweeper	Darktrace			Verinice	Parrot Sec	P&V SIEM				XX		
68	Capacity management is not in place and from what is seen XXXXX does run without 35% unused security capacity	Servicing	Asset Management	LanSweeper				Verinice	Parrot Sec	P&V SIEM		2			XXX	Ext.
69	Data can be accessed on RHEL servers via SMT without permission for is. Patching required.	Servicing	Patch Management	LanSweeper	Darktrace			Verinice	Parrot Sec	P&V SIEM		1		XX		Int.
70	Endpoint none standard images	Servicing	Asset Management	LanSweeper				Verinice	Parrot Sec	P&V SIEM		15			XXX	Mix 50-50
71	IE: unauthorized Active X controls (Very high Risk) 15.809	Servicing	Patch Management	LanSweeper	Darktrace			Verinice	Parrot Sec	P&V SIEM		1		XX		Int.
72	Mule soft runtime allows directory hopping - patch must be installed	Servicing	Asset Management	ABC	Syslog Analyser			Verinice	Parrot Sec	P&V SIEM		1	X			Int.
73	*NASD 10 but only 7 are known*	*Servicing*	*SIR unite should be a fully segregated & independent network*	*LanSweeper*	*Darktrace*			*Verinice*	*Parrot Sec*	*P&V SIEM*		*1*	*X*			*Int.*
74	No monitoring of hosted storage, application	Servicing	Asset Management	ABC	Syslog Analyser			Verinice	Parrot Sec	P&V SIEM		2	X			Mix 50-50
75	No monitoring, scanning, activities logging of business critical servers; e.g. exchange, file, DC, …	Servicing	Asset Management	ABC	Syslog Analyser	Exchange Auditor	Lansweeper	Verinice	Parrot Sec	P&V SIEM		10	X			Mix 50-50
76	Since April 2015 no Java (v5, v6 and v7) security updates have been installed due to out-ofsupport. Ao V-Connect, Tango and EB-connect are impacted. CVSS score 10 -> jQuery 1.4.4 reached endof-life in 2016-05-20 and is no longer supported by the vendor	Servicing	Patch Management	LanSweeper	Syslog Analyser			Verinice	Parrot Sec	P&V SIEM		1		XX		Int.

77	The high amount of versions of individual application does indicate a non-existing or badly managed software deployment & patch management.	Servicing	Asset Management	LanSweeper	Darktrace			Verinice	Parrot Sec	P&V SIEM		6			X X X	Resolved by N° 75
78	Upgrade to version 1.1.0i, 1.0.2p, 1.1.1 or later of OpenSSL - 1 target	Servicing	Patch Management	LanSweeper	Syslog Analyser			Verinice	Parrot Sec	P&V SIEM				X X		Int.
79	Upgrade to version 2.4.35 or later of Apache HTTP Server - 1 target	Servicing	Patch Management	LanSweeper	Syslog Analyser			Verinice	Parrot Sec	P&V SIEM				X X		
80	Upgrade to version 7.2.12, 7.1.24, 7.0.32, 5.6.38 or later of PHP - 1 target	Servicing	Patch Management	LanSweeper	Syslog Analyser			Verinice	Parrot Sec	P&V SIEM		6		X X		
81	Vulnerability for remote executions via RDP without the necessary credentials have. CVE-2019-1181 and CVE-2019-1182	Servicing	Patch Management	LanSweeper	Syslog Analyser			Verinice	Parrot Sec	P&V SIEM				X X		
82	Vulnerability for WannaCry (SMBv1) has been determined during a Checkpoint study. Protocol connected to Win2008 (file share) solutions.	Servicing	Patch Management	LanSweeper	Syslog Analyser			Verinice	Parrot Sec	P&V SIEM				X X		
83	Windows error events generated 507.652	Servicing	Asset Management	LanSweeper	Syslog Analyser			Verinice	Parrot Sec	P&V SIEM					X X X	Resolved by N° 75
84	4 different Workgroups in the XXXXX network	Servicing	NAC	LanSweeper	Darktrace			Verinice	Parrot Sec	P&V SIEM			X			Resolved by SOC
85	None controled and cleaned Backups - DRP	Servicing	DRP - BCP	This should become part of the RFP N° 58											X X X	
86	FTP servers that are externally connected are detected	SOC	Network	ABC				Verinice	Parrot Sec	P&V SIEM				X X		Resolved by SOC
87	Get a view on file exchanges with other companies through batches, fpt, sftp, mail : data flows are often not encrypted and uncontrolled	SOC	Network	ABC				Verinice	Parrot Sec	P&V SIEM				X X		
88	HTTP (TCP port 80) - https	SOC	Network	ABC				Verinice	Parrot Sec	P&V SIEM			X			Can be directly resolved with the Firewalls
89	https traffic only, also internal	SOC	Network	ABC				Verinice	Parrot Sec	P&V SIEM			X			
90	Revue secured IP/DNS mgmt.	SOC	DDI	ABC	Verinice			Verinice	Parrot Sec	P&V SIEM		10		X X		
91	CASB to get a grip on data leaking to the cloud	SOC	Network	ABC				Verinice	Parrot Sec	P&V SIEM		6		X X		Ext.
92	Implementation on site of ABCD	SOC										5		X X		Ext.
93	Implementation on site of ABCDE Plus	SOC										10		X X		Ext.
94	Implementation on site of Exchange Auditor	SOC										10		X X		Ext.
95	Implementation on site of SysLog Analyser	SOC										10		X X		Ext.
96	Implementation on site of Security Onion	SOC										10		X X		Ext.
97	Implementation on site of Verinice	SOC										60		X X		Ext.
98	Implementation on site of Centrify	SOC										10		X X		Ext.
99	Implementation on site of Ninoseki/Mihari/TheHive	SOC										10		X X		Ext.
100	Finetune ABC	SOC										5		X X		Ext.

3 c Maturity Model - Annex 3

The Core

The core idea of O-ISM3 is that information security is not just about the prevention of attacks to information systems, it is about achieving the organisation's mission despite attacks, accidents and errors. There is no alignment between security objectives (the traditional confidentiality, integrity, availability) and business goals; but in O-ISM3, they are one and the same. If a company makes pastries, quality would be to deliver pastries that customers find tasty for the price they are willing to pay, while security would be to continue delivering pastries despite accidents (fire, earthquake), attacks (denial of service, viruses) and errors (administrator or operator error).

This core idea leads to defining confidentiality, availability, integrity and related concepts in great detail. O-ISM3 security objectives depend on technical, business and compliance needs and limitations. For example, the requirements of an invoicing system can be specified as follows using O-ISM3:

- Invoices should only be accessible to the accounting and collection departments.
- Paid invoices are to be kept for three years and destroyed after no more than four.
- The invoicing system has to register the user account at the date and time of creation, and needs to be available 9 a.m.-5 p.m. Monday through Friday, with no more than five interruptions per week, and a duration of no more than one hour in total, and cause no more than 15 Invoices to be re-entered.
- There must be less than five errors per hundred invoices. More than 99.8 percent of products served must be invoiced.
- Since the invoicing system is a third-party application, the license must be kept current.
- As the invoicing system keeps personal information, according to the law, the database must be registered at the Data Protection Agency. The invoicing system must not be visible to systems from outside the company or have any remote access. It must be kept in the Data Center under controlled environmental conditions and company safeguards against fire, flood, etc.
  Implement TOGAF and SABSA architectures.

Maturity Levels

The second main concept of O-ISM3 is designing the system using maturity levels. Having maturity levels (ISM3 has five) helps organisations that can only afford to invest 20 percent, achieving 80 percent of results, (this is the 80/20 rule). The highest return from security

investment comes from the initial investment, as the Mayfield's paradox and a study from Carnegie Mellon. Different levels of maturity let organisations choose a baseline for their initial Information Security Management (ISM) system, and use the rest of the levels as milestones to higher (and more resource-consuming) O-ISM3 levels as the organisation evolves. With maturity levels the organisation can prioritise investment and measure progress. CMMI and ISO 14001 are examples of standards that use maturity levels.

Process vs. Controls Orientation

Using a process-oriented approach toward ISM is another main idea. The principle followed is, "What you can't measure, you can't manage, and what you can't manage, you can't improve." O-ISM3-based management systems are based on processes with well-defined outputs that can be measured. This allows for a continuous improvement of the processes, as there are criteria to measure the performance of the ISMS. ISO 9001, COBIT and ITIL use a process-oriented approach.

The focus of O-ISM3 management is not limited to risk assessment and audit. O-ISM3 process orientation covers the following management activities:

- Risk assessment—Consider assets, threats, vulnerabilities and impacts to get a picture of security, and prioritise design and improvements.
- Audit—Compare the actual management system with the documented management system.
- Compliance audit—Compare the actual management system with a externally defined management system (e.g. ISO 27001).
- Monitor—Use metrics to watch processes outputs, detect abnormal conditions and assess the effect of changes in the process.
- Test—Check if inputs to the process produce the expected outputs.
- Design and improvement—Find ways to produce outputs better fit to their purpose, fewer false positives and false negatives (including faster outputs).
- Optimization—Find ways to produce the same outputs with fewer resources.

This helps chief information security officers (CISOs) to manage their ISM systems when an audit is not under way.

Processes and controls are different, but both can be tested by auditing them. Processes' results are defined (outputs), so it is very clear what to do to implement the process and the process can be improved using the process metrics. On the other hand, controls do not have a defined result, which makes them less management friendly, as a malfunctioning control does not produce information (results) necessary to learn what went wrong and take a management decision to fix it.

Controls are associated with an objective. For example, the question “What is the objective of a firewall?” has an answer: “To protect the perimeter of a network.” The next logical question in sequence is to check whether or not the objective is fulfilled by asking, “What is the result of using a firewall?” This can be answered only by measuring the result of a process which uses the firewall. By implementing processes, information security becomes more wholesome and holistic. The focus shifts from the control to the whole environment.

Metrics

Information security processes are manageable using metrics. This lets managers show the results, how results benefit the organisation, and check what changes in the process make the process improve and by how much. It also facilitates accountability.

It seems common sense that there is a direct link between what the organisation does (outputs) and what the organisation wants to achieve (goals). This belief is supported by reallife experiences, for example making a cheese sandwich. One buys the ingredients, goes home, arranges them, and perhaps toasts them, voilá: a warm cheese sandwich ready to eat. The output, cheese sandwich, and the goal, eating a homemade cheese sandwich, match beautifully.

Unfortunately, common sense fails more often than expected. A good example is research. The goal (i.e., discovery) and the activity (i.e., experiments, documentation) are not directly linked. One can try hundreds of experiments and still not find the answer. The same thing happens with security. The goals (i.e., trust, confidence, risk) and the activity (i.e., controls, processes) are not directly linked. For this reason O-ISM3 emphasises measuring what one can control, the outputs of one’s processes, specifically:

- Activity: The number of outputs produced, their mean age, the mean time between outputs submissions, mean time to produce an output, following input, and worst case time to produce an output, following input.
- Scope: The proportion of the environment or system that is protected by the process and the percentage of the scope sampled.
- Unavailability: The time since a process has performed as expected upon demand (uptime), the frequency and duration of interruptions.
- Effectiveness: Number of inputs, mean time between inputs, and percentage of inputs that produce an output.
- Efficiency: Ratio between the number of outputs submitted and the available resources for this process in actual use.
- Load: Percentage of resources in actual use.
- Quality: Accuracy, precision, or other measurements of fitness for purpose of the output, when applicable.

Results of processes within O-ISM3, called “outputs” are defined. For example, in the case of the access control process, the expected outputs of the system could be defined as:

- Grant of access to authorized users;
- Denial of access to unauthorised users;
- Logs of password changes;
- Logs of authorised access to information; Unauthorised access attempt reports.

The process could be tested in two ways. The first method is similar to testing the control, but this would reflect only the current state of the system. A more comprehensive way to test the process is to measure the results of the process by using the metrics.

From the above metrics, the values obtained under scope and availability would be used to improve security directly, and those obtained under activity and update would be used indirectly to improve security by improving the process. For example, if 100 access rights are normally granted every month, but in one month it is noticed that only 10 access rights were granted, an investigation of the process would be appropriate.

This could indicate different scenarios. Either people are not asking for access rights any longer and are sharing them, the person responsible for the access control system is not doing his/her job properly, or the second condition could be the cause of the first condition.

A common problem with metrics is finding criteria that tell when the metrics deserve attention. O-ISM3 recommendations are borrowed from quality management, using control charts. Control charts help managers distinguish simply random, important changes from noteworthy abnormalities that should be investigated.

O-ISM3 and Other Standards

O-ISM3 protects existing investment in ISM systems, as O-ISM3 describes processes in such a way that current practices can be easily adapted to O-ISM3 requirements.

ISO 9001 users will find that O-ISM3’s document management requirements are the same; the same document management system can be used to handle ISO9001 and O-ISM3 documents. The PDCA principle used in ISO 9001 is used extensively in O-ISM3, and if familiar with ISO9001 management principles, that knowledge can be used for ISM systems. (The PDCA principle is used by O-ISM3 in a process-by-process fashion, not just for the whole ISM systems.) O-ISM3 recommends the use of control charts for the interpretation of O-ISM3 metrics.

COBIT users will find that the O-ISM3 concept of security fits naturally with security, quality and fiduciary requirements. key goal indicators (KGIs) and key performance indicators

(KPIs) can be measured by using O-ISM3's metrics The level of detail that OISM3 brings can make ISM system design easier.

Although ITIL process approach is congruent with O-ISM3, ITIL security management is not very specific. O-ISM3 can reinforce ITIL's ISMS practices, and setting metrics thresholds is probably the best way to specify underpinning contracts and service level agreements.

There is a natural fit between O-ISM3's business goals, security objectives (technical, business and compliance objectives) and IT governance concepts. O-ISM3 uses a clear division of responsibilities between leaders, managers and technical personnel by using the concepts of strategic, tactical and operational management. Strategic managers are involved with the long-term alignment of IT with business needs. Tactical managers are involved in the allocation of resources and configuration and management of the ISM system. Operational Managers are involved in setting up, operating and monitoring the operational (technical) processes. In the implementation of O-ISM3, it is easy to determine security responsibilities due to the division of the O-ISM3 processes. This division represents a way of thinking about what results are to be achieved and to whom the results will be reported.

O-ISM3 is ISO 27001-compatible to the point that O-ISM3 can be used as a tool to aid the implementation of ISO 27001 or to certify an organisation by both standards. O-ISM3 is a specification for creating ISM systems, so O-ISM3 itself does not need to be ISO27001 compliant. Certification is performed on specific ISM systems, thus O-ISM3 can be used to create ISO 27001-compliant ISM systems that will have to use risk analysis/assessment and implement all applicable ISO 27001 controls. The O-ISM3 Consortium provides certification in collaboration with ISO 9001 and ISO 27001 certification bodies.

O-ISM3 provides a risk analysis methodology, which is compatible with the use of all widely recognized risk analysis standards, like OCTAVE, MEHARI, EBIOS or MAGERIT.

Certification of ISM systems is very important, as organisations use certification to show their commitment to information security and build trust relationships. An ISM system based in O-ISM3 is creditable under ISO 9001 or ISO 27001 schemes, which means that O-ISM3 can be used to implement an ISO 27001-based ISMS.

Conclusion

If an organisation already has an ISM system in place, O-ISM3 is compatible with this approach, and can help enhance current ISM systems beyond compliance with current standards to higher, and more difficult to achieve, maturity levels. If an organisation does not yet have an ISMS and is familiar with process-based management approaches such as ISO 9001, COBIT or ITIL; if an organisation needs a top-down approach that roots on its business mission; if the organisation has limited resources; or if the organisation plans to outsource parts of its ISMS or is looking for an accredited ISM system, then O-ISM3 is right for the organization.

3 d Maturity Model Roadmap - Annex 4

Active Directory MRM	C1	C2	C3
	Status %		
	54.78	60.39	91.28

Servicing MRM	C1	C2	C3
	Status %		
	42.85	81.41	94.21

SOC MRM	C1	C2	C3
	Status %		
	57.23	84.46	97.84

The Core & Cisco & CIO are linked to either and RFP and / or to organisational changes and by so the MRM cannot be valued unless a clear timeframe is being communicated for this study.

3 e Tools Description - Annex 5

3 f SOC / Capex – Opex - Consultancy - Annex 6

3 g Project Consultancy - Annex 7

3 h Implementation 3 years mapping - Annex 8

Area	Sep-19		Sep-20		Sep-21		Sep-22	
	Operational Level	*Security Level*	*Operational Level*	*Security Level*	*Operational Level*	*Security Level*	*Operational Level*	*Security Level*
IT internal security concerns								
IT external security concerns								
Information Security Risk Management								
Information Security Incident Management								
Compliance GDPR / NIS								
Operations Management								
Asset Management								
Business Continuity Management								
Physical and Environmental Security								
Security Policy								
Human Resources								
Organising Information Security								

The above rankings are evolving based up on the projects, roadmap and findings ranking established by XXXXX. As some issues highlighted by CPE-DRS have been ranked as out of scope or to be analysed, as they cannot be associated to any XXXXX projects the ponderation has changed. It is also essential to highlight that resolution of the CPE-DRS findings do not include any evolution of none covered issues by the audit but that are cross-linked to the findings. The tables does only include the situational snapshot of September 2019 and its eventual evolution. Anything out of the 99 highlighted concerns cannot be taken into concern in the above evolution table.

3 i XXXXX findings ranking - Annex 9

3 j Update Internal Scan - Annex 10