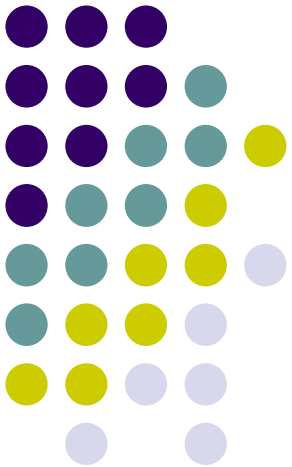
Sistem Manajemen Keamanan Informasi (SMKI)

Bayu Setyatmoko, ST., MT., MTCNA, CEH

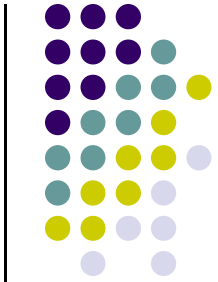
(Email : bayusetyatmoko@gmail.com)

Bidang Persandian Diskominfo Pati



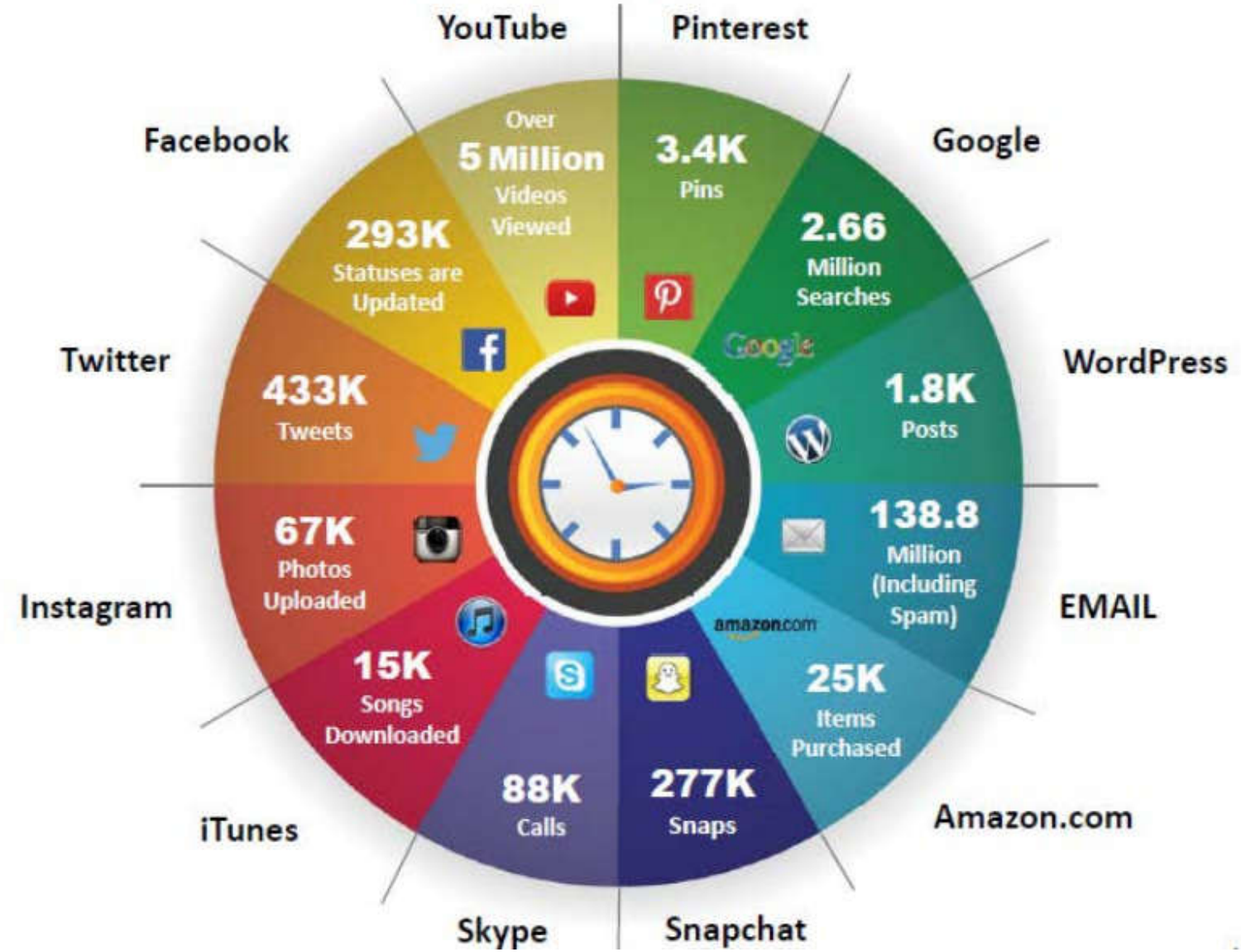
Pati, 20 Nopember 2017

Agenda



- Digital Life Style
- HAM Radio & Digital Mode
- Anatomy of Hacking
- Aspek Keamanan Informasi
- Cyber Security Stack
- Peta Tata Kelola SMKI
- Aspek Tata Kelola SMKI
- Indek Keamanan Internet Domain Indonesia (KIDI)
- Government Chief Information Officer (GCIO)
- Paradigma Baru Persandian
- Regulasi Bidang Persandian

Digital Life Style



The HAM Radio

ICOM 7000
$1,265.00 (HF, VHF, UHF)

Yaesu FT-817ND
$699.00 (HF, VHF, UHF)

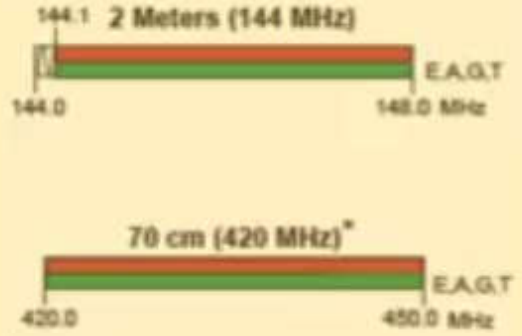
ICOM 718
$729.00 (HF Only)

Yaesu FT-857D
$849.00 (HF, VHF, UHF)

Kenwood TS-2000
$1,454.00 (HF, VHF, UHF)

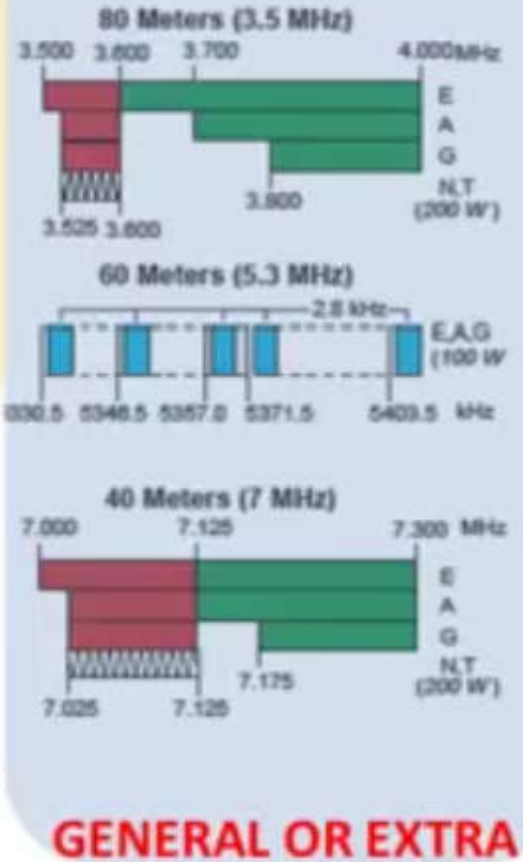
Frequency Range

LOCAL



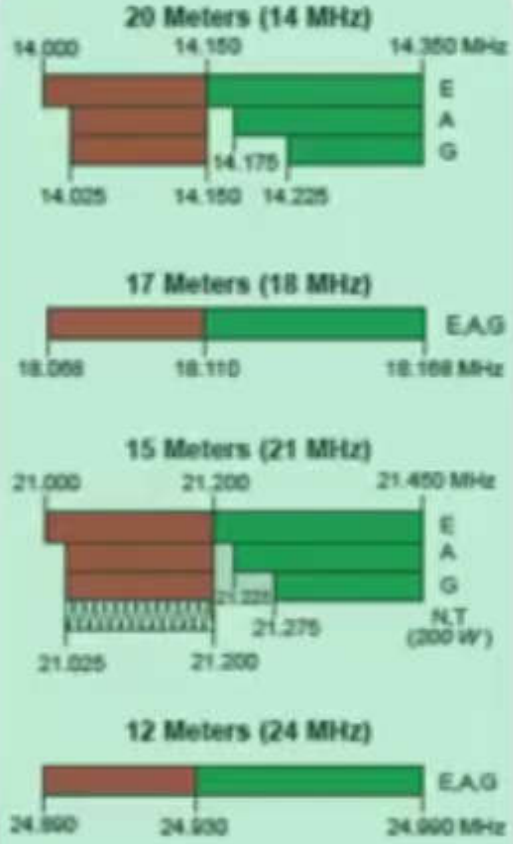
TECHNICIAN CLASS

REGIONAL



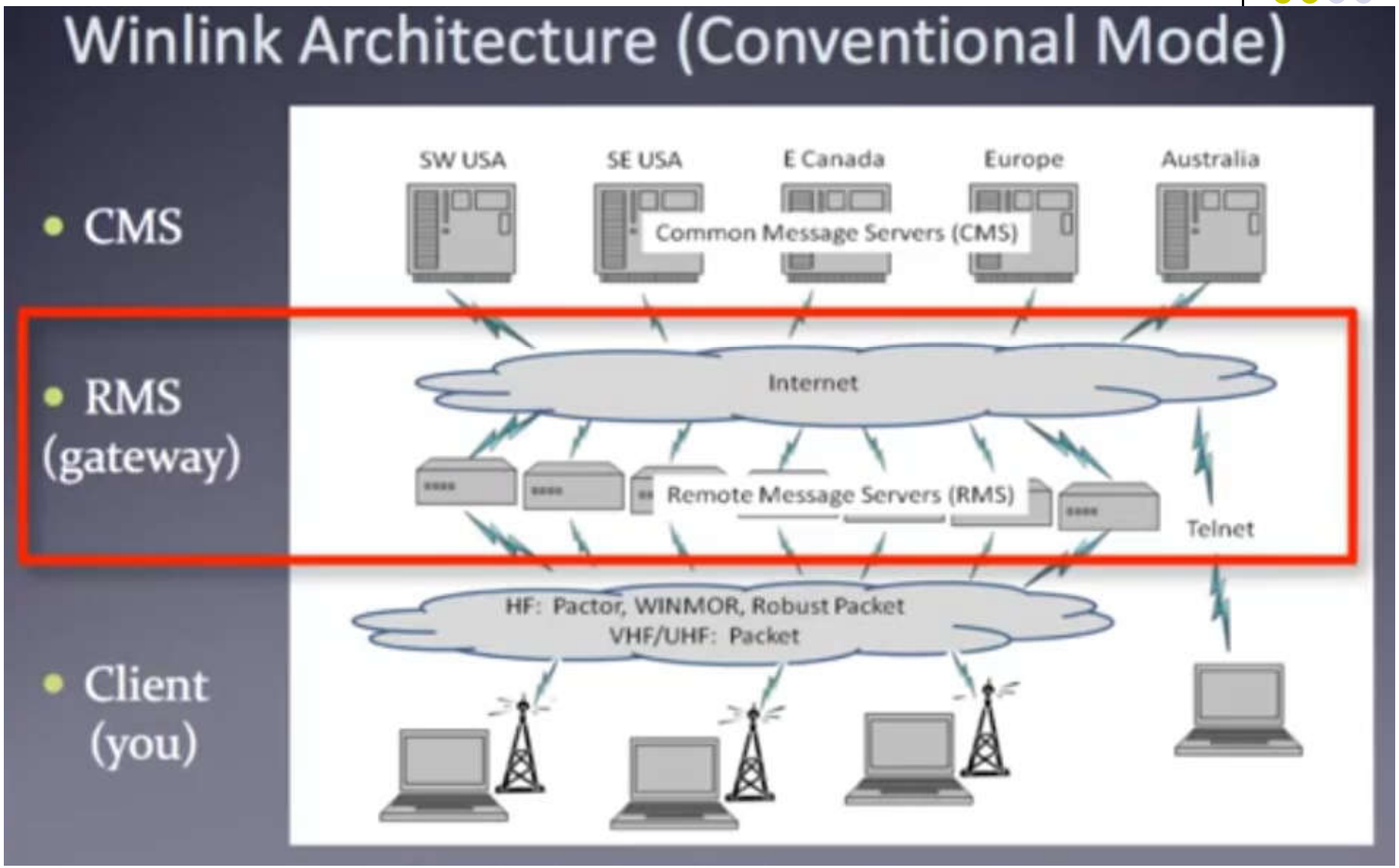
GENERAL OR EXTRA CLASS

INTERNATIONAL



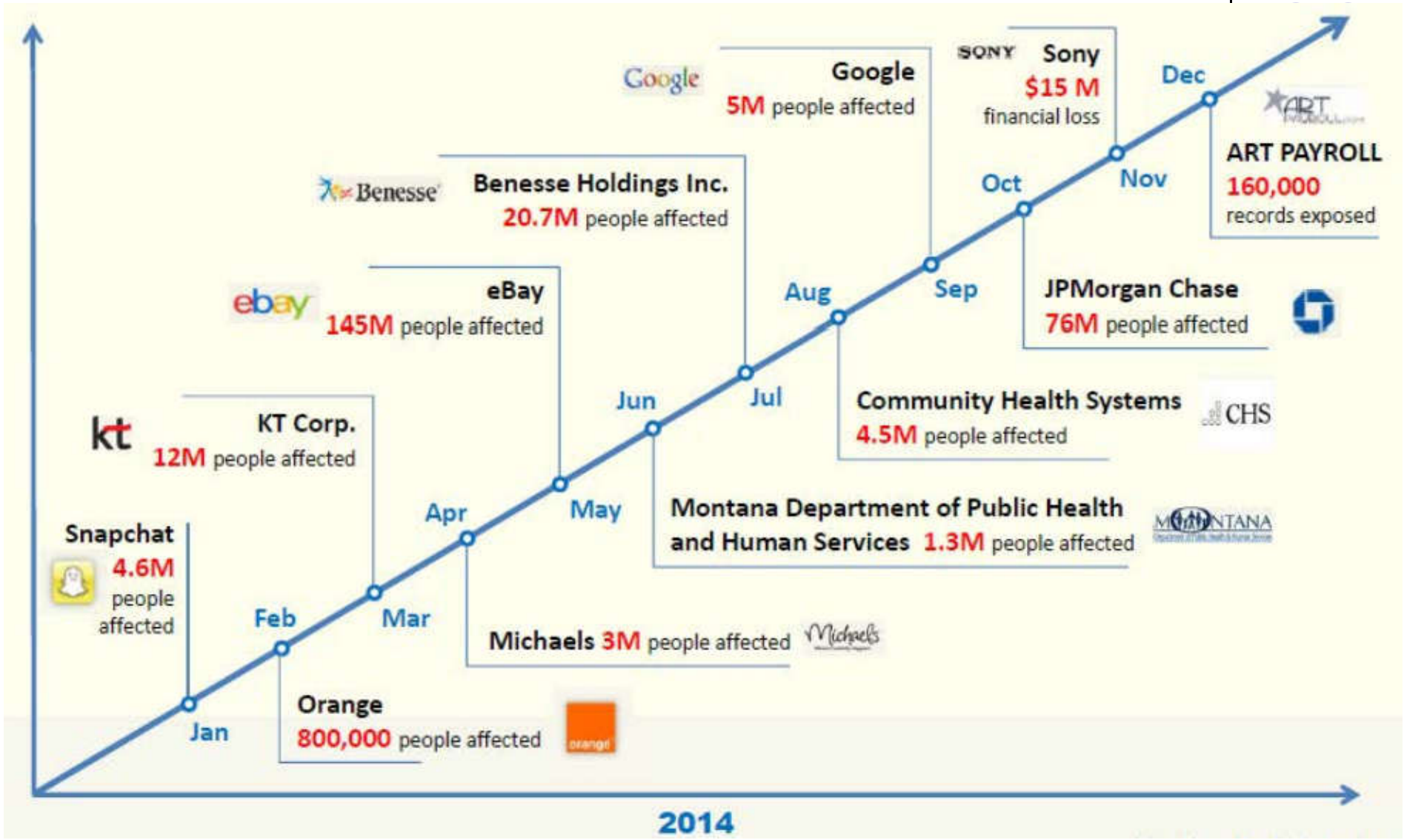
GENERAL OR EXTRA CLASS

Digital Mode (Winlink)

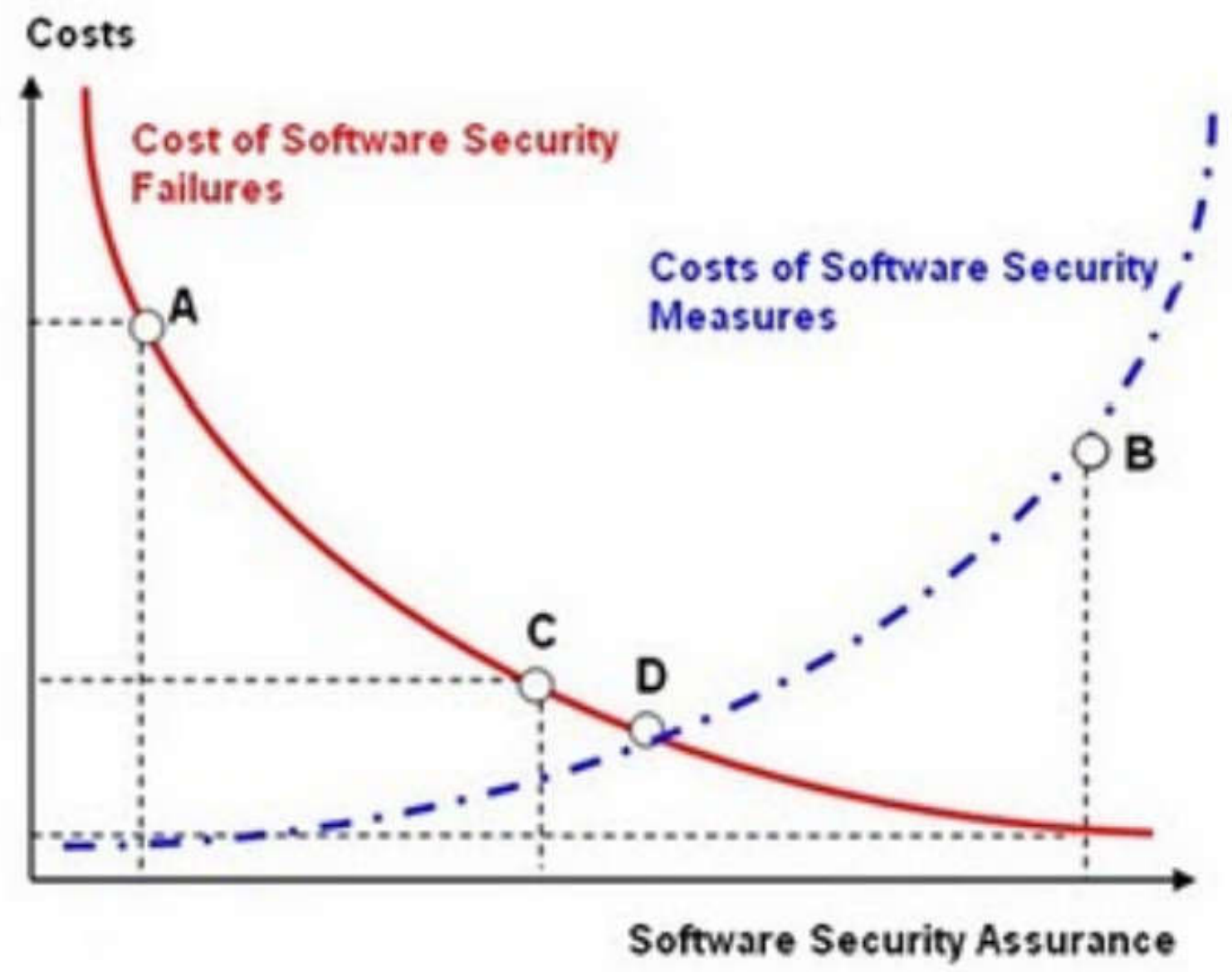


ICOM (Digital Mode)

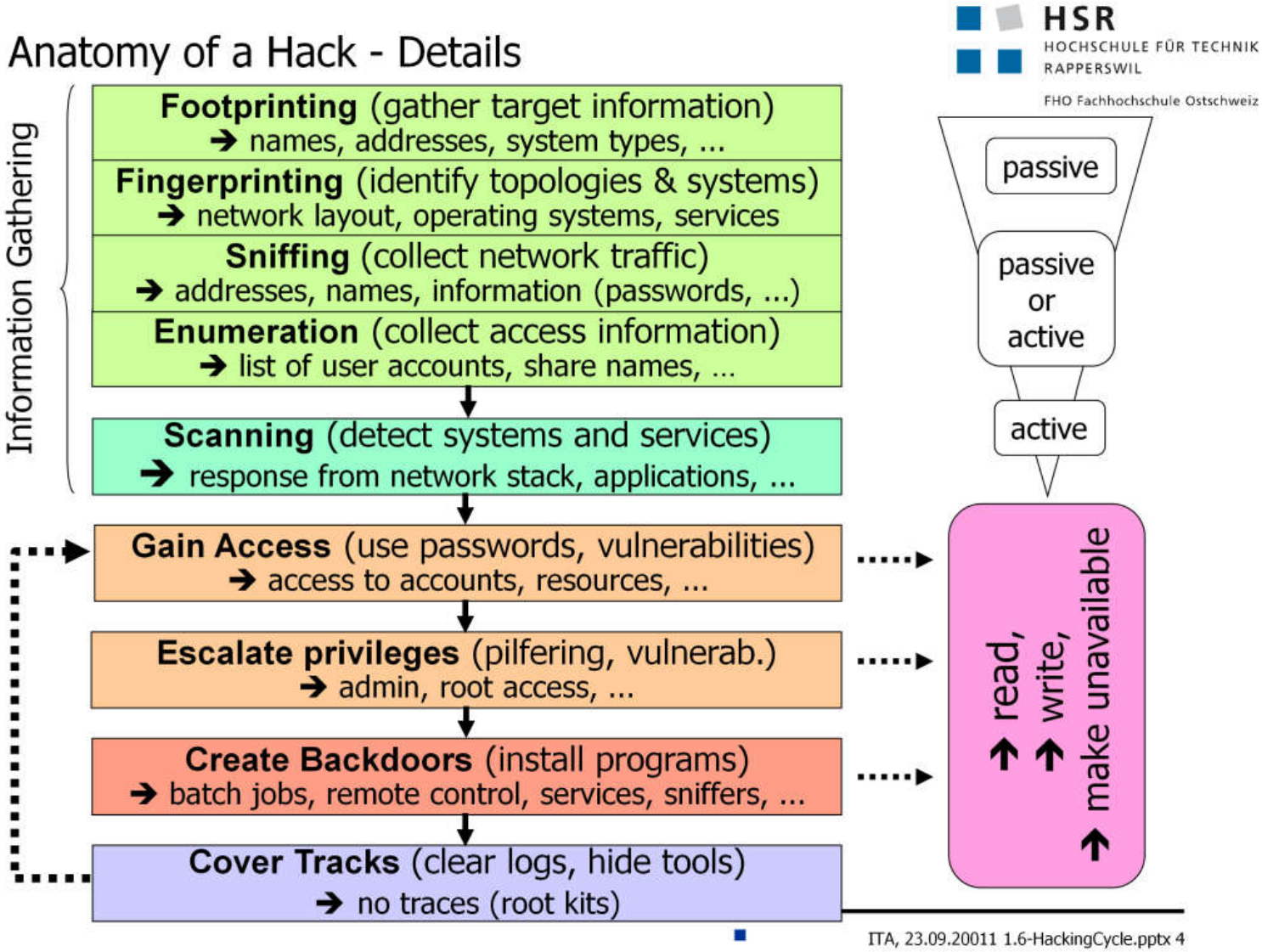
Mega Breach 2014



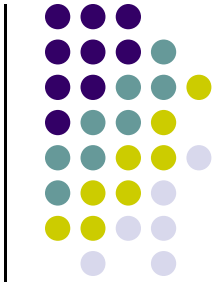
Cost vs Security Assurance

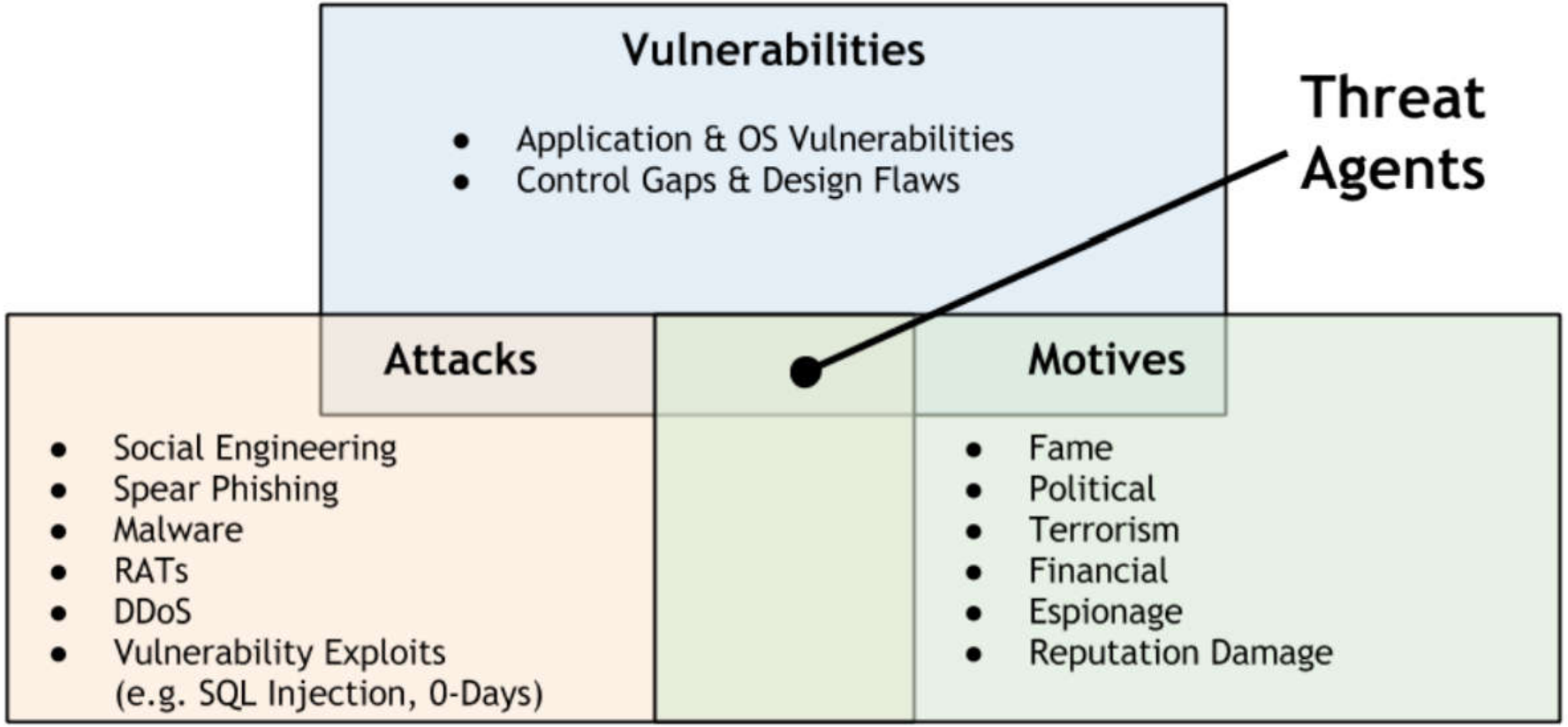


Anatomy of Hacking

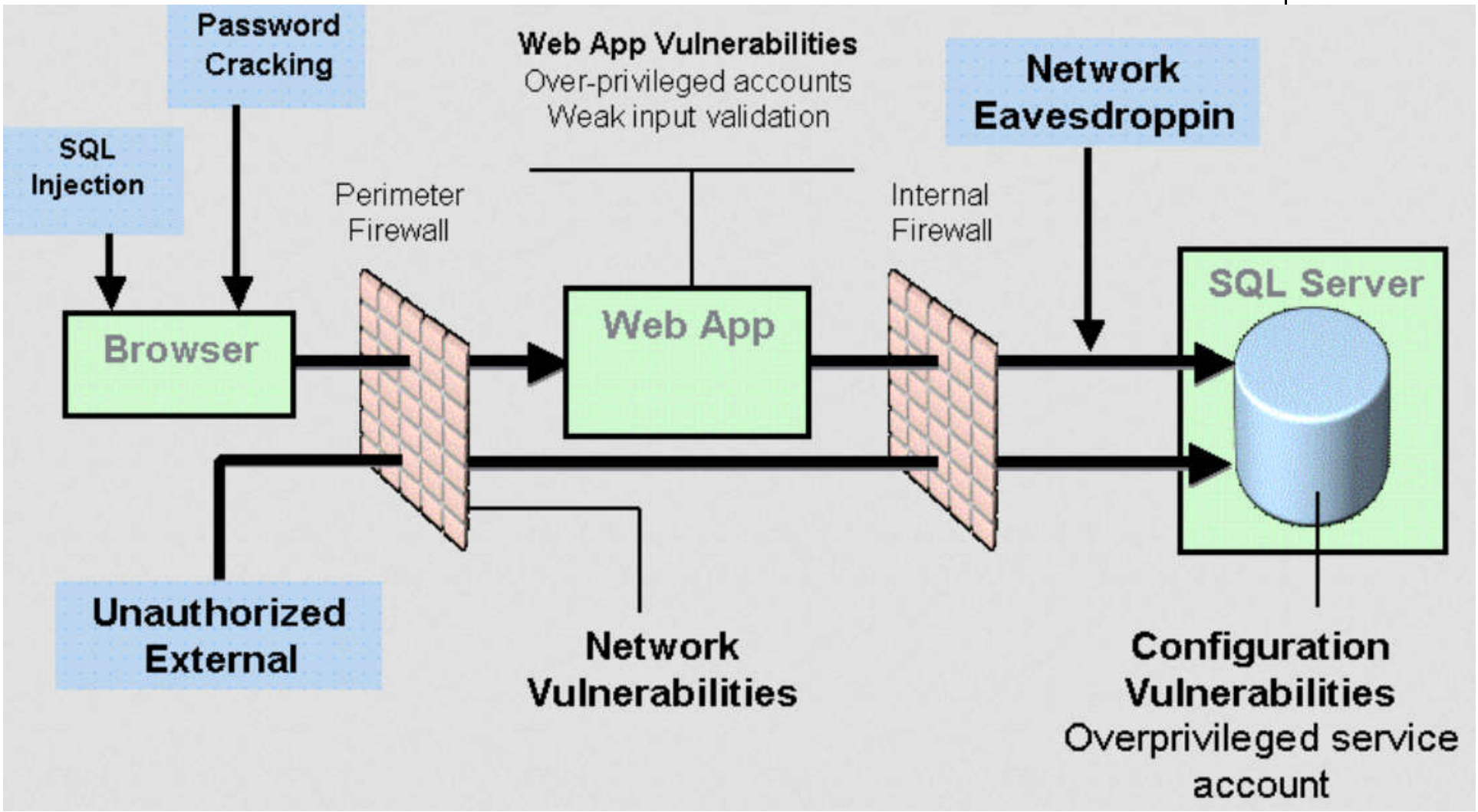


Threat Agent

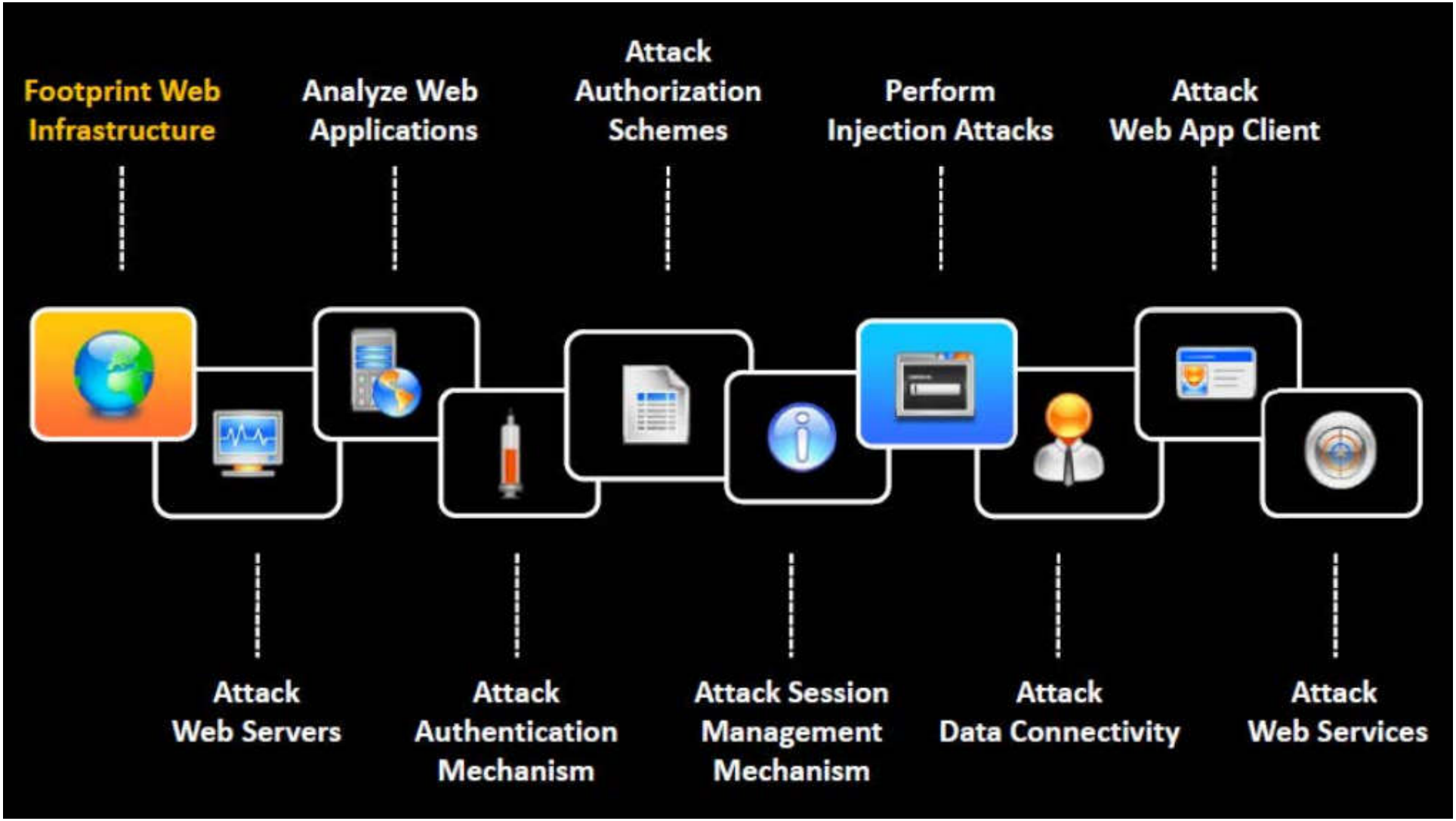




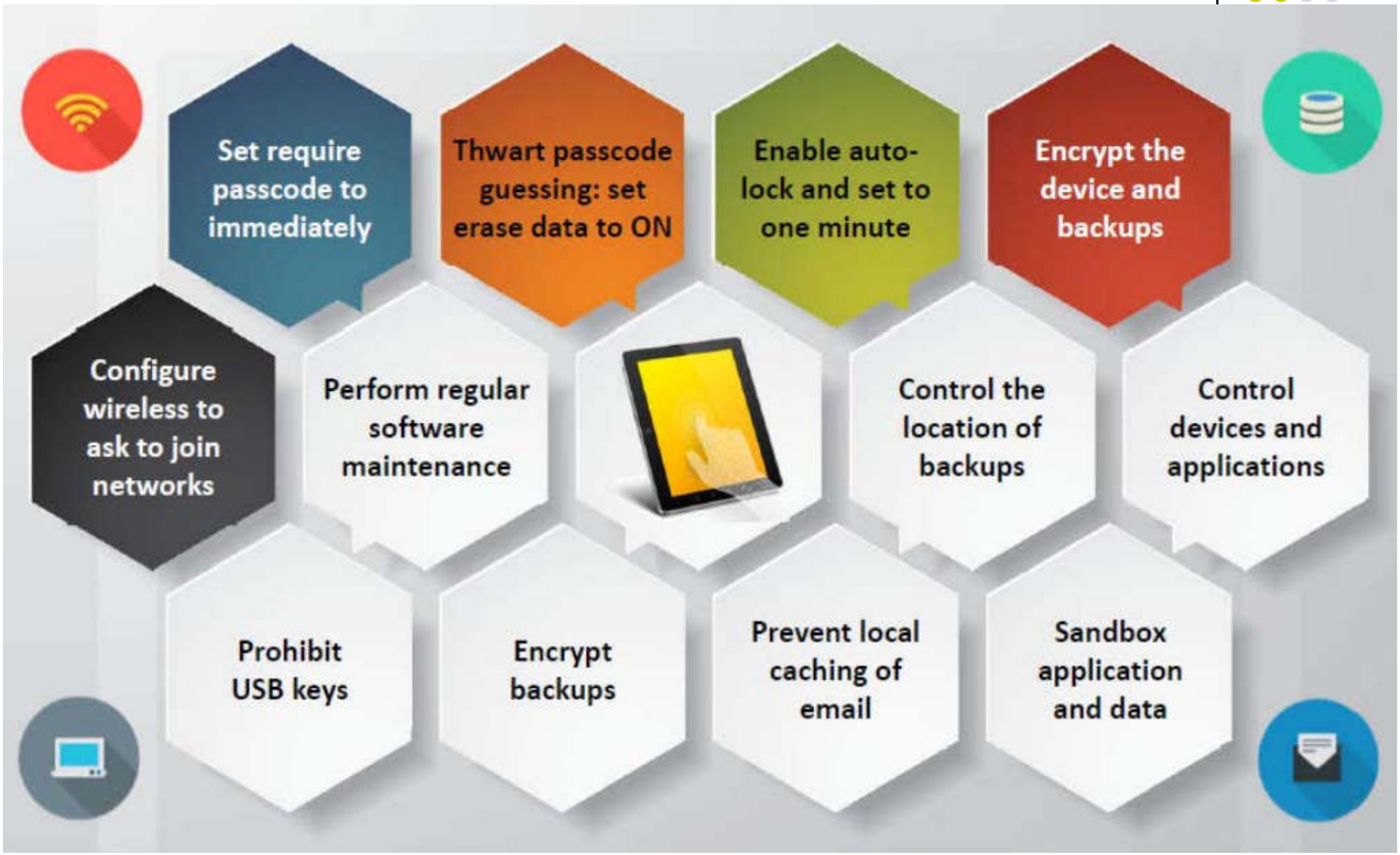
Website Security Threat



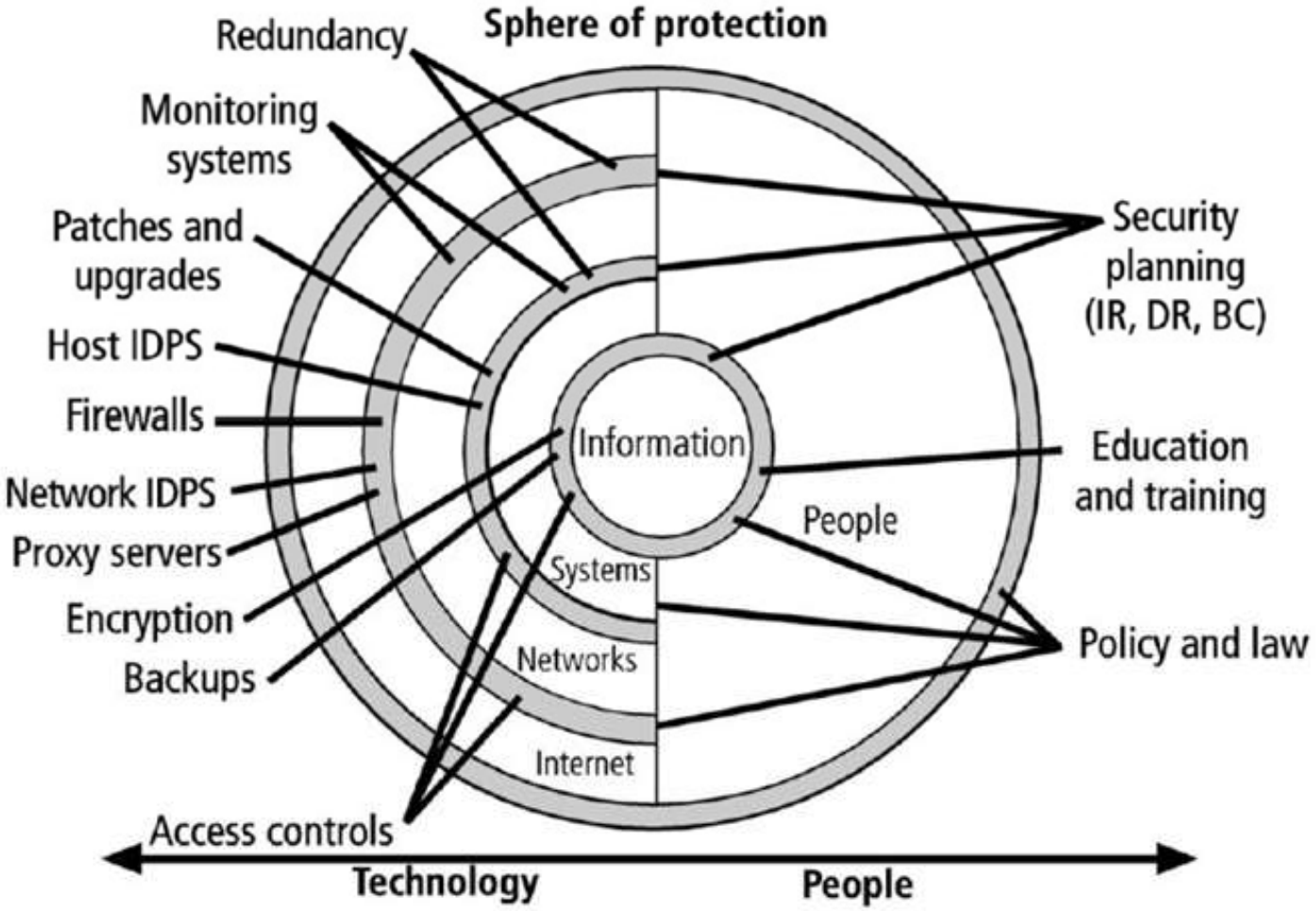
Stage of Website Attack



Securing Android Device

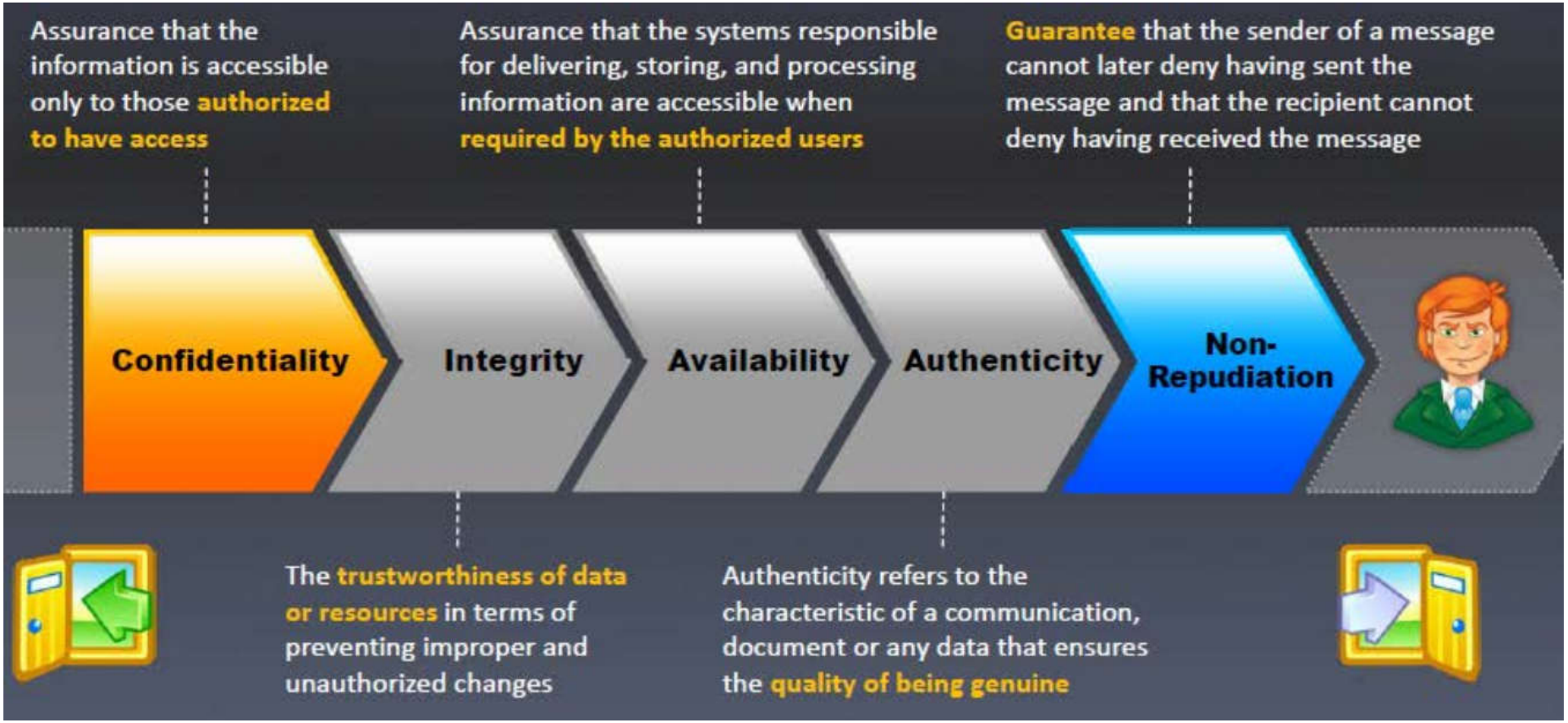


Aspek Keamanan Informasi

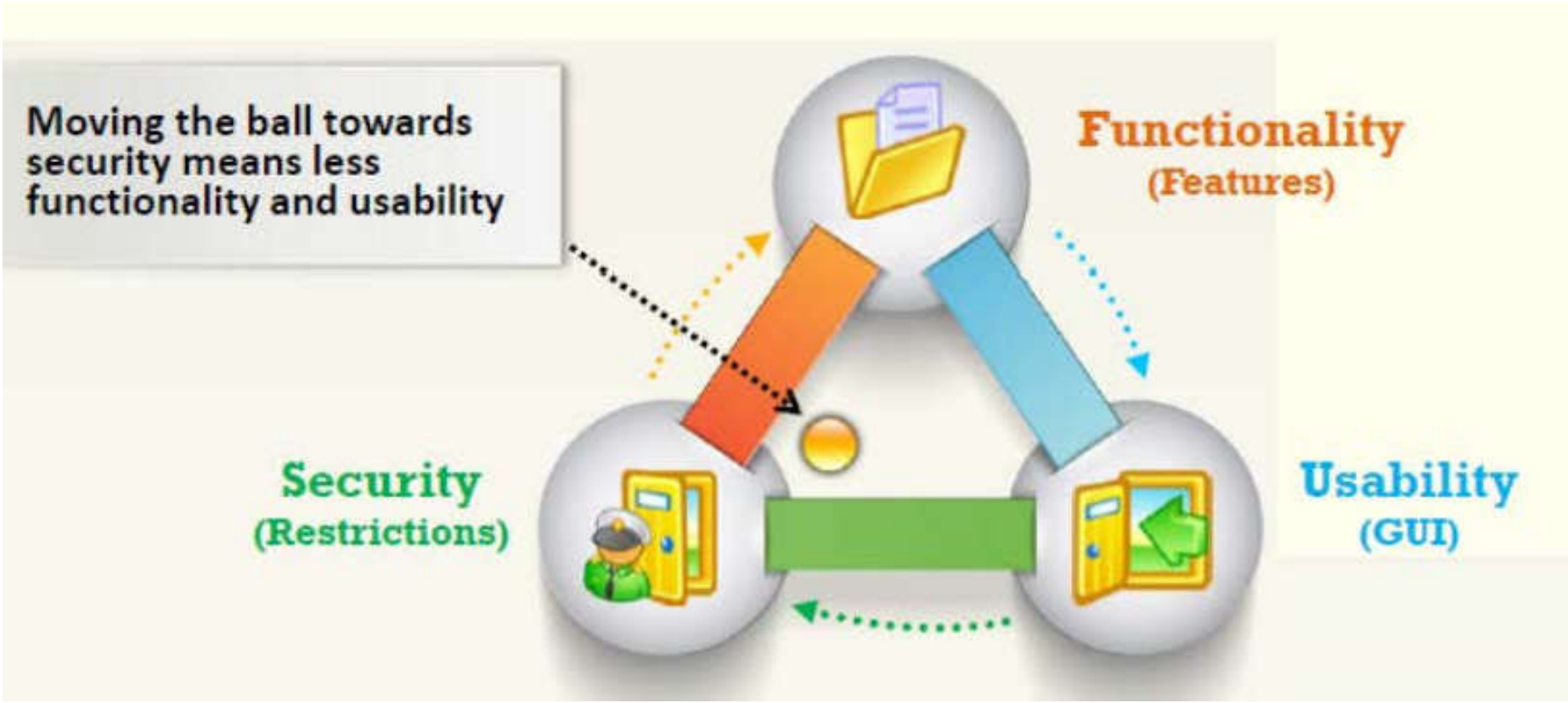


"There is no security patch for human stupidity"

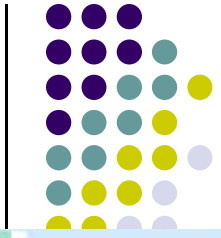
Elemen Keamanan Informasi



Level of Security



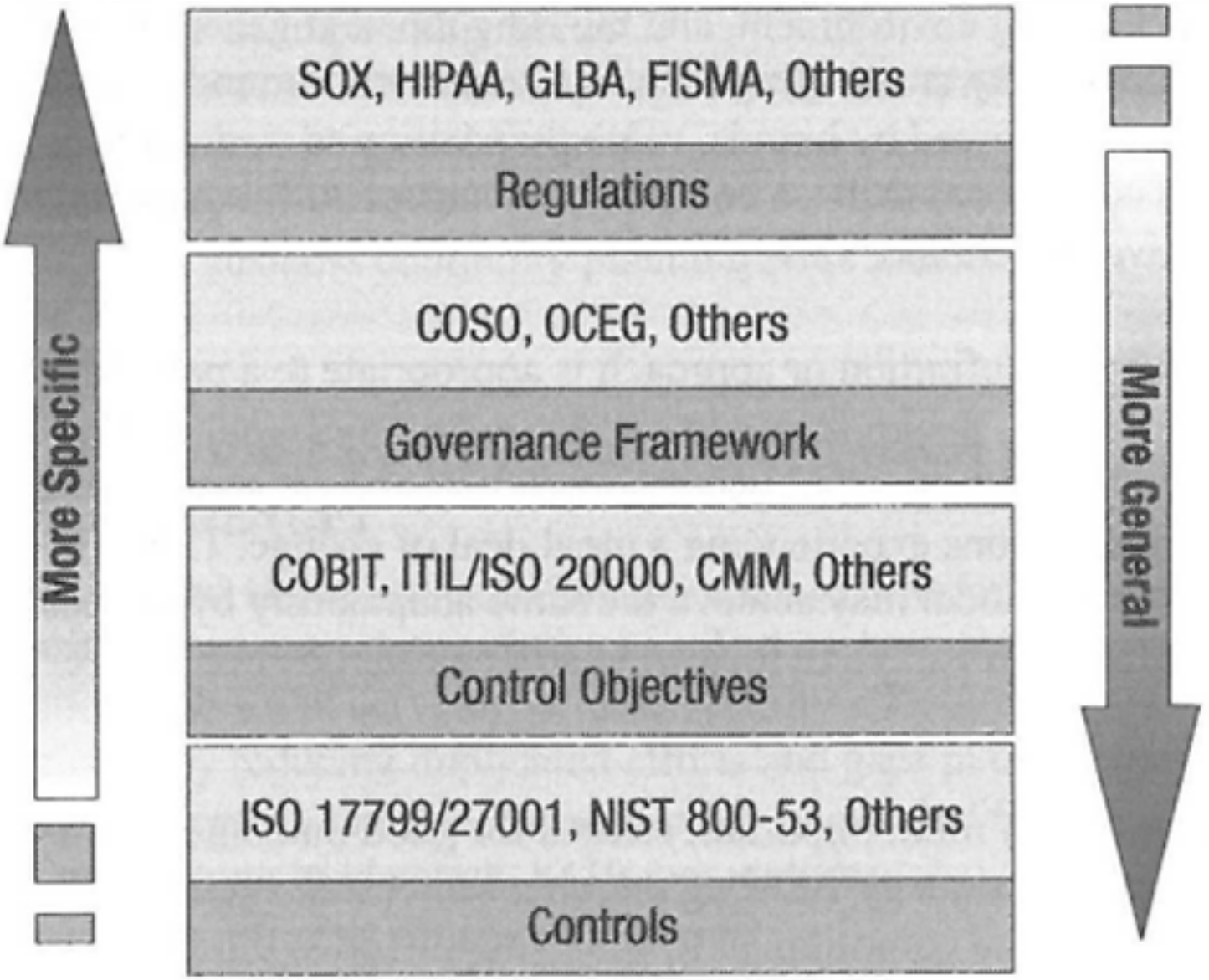
Cyber Security Stack



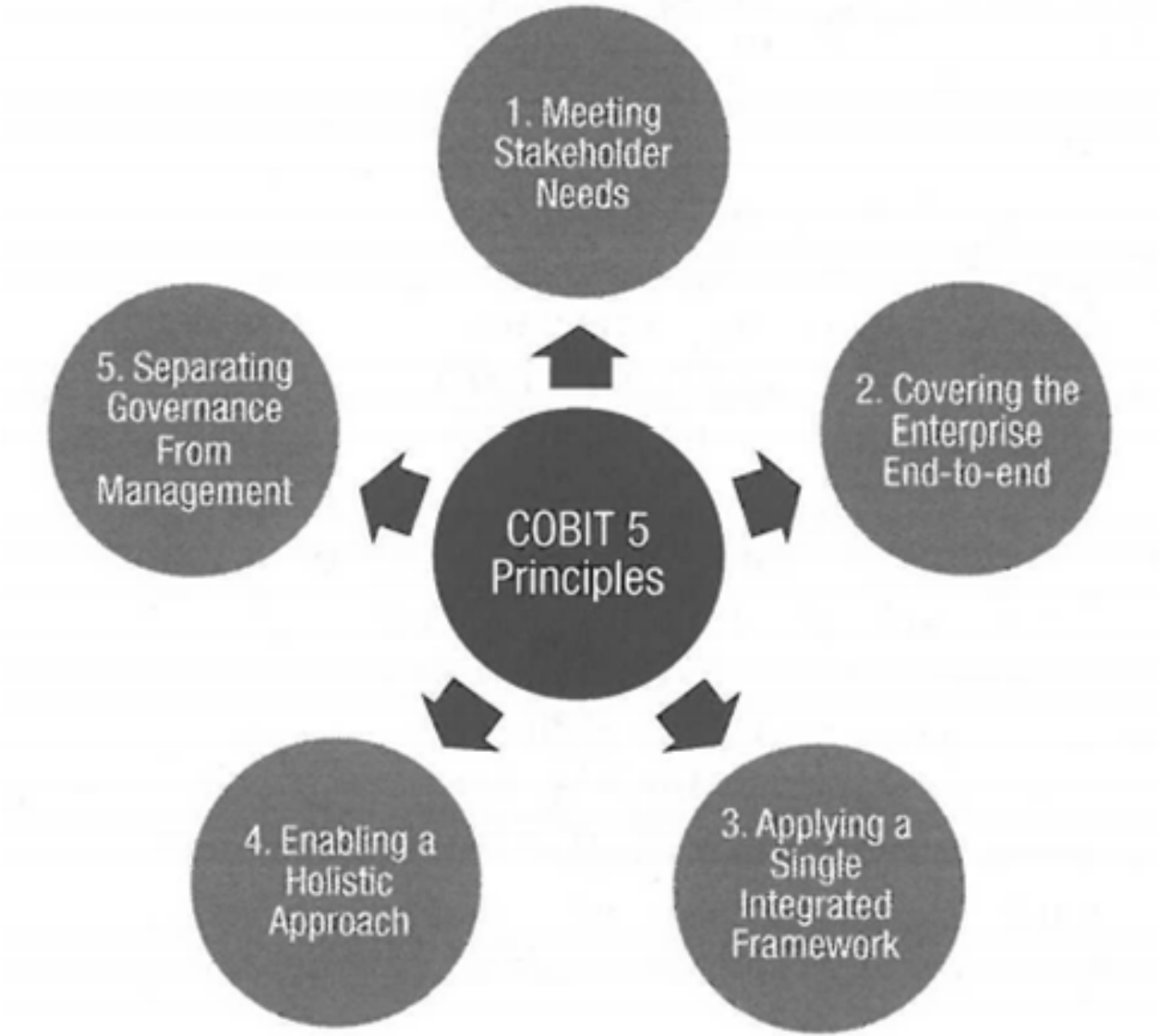
Process	Vendor Security Assessment	Security Policy Management	Control Automation	Risk Management	Training & Communicatio n	Compliance Adherence	Mobile business	
People	Privileged User Password Management	Roles & Entitlements	User Access Managemen t / Monitoring	Access Reviews & Attestations	Federation & SSO	Identity Theft	Threat – Insiders & Outsiders	
Data	Data Loss Prevention	Information Exchange (IRM)	Content Security	End Point Protection	Data Protection Directives	Data Loss - Social Networking	Sensitive Data Vaulting	
Infrastructure	Host Intrusion Detection and Prevention	Network & Perimeter Security	Data Loss Prevention	Intrusions (viruses, worms)	Production / Non production Data Masking	Security Monitoring	Cyber threats / warfare/APT's	Cyber Analytics
Applications	Secure Design Review	Security Source Code Consulting	Pre Dev Security Assessment	Threat & Vulnerability Managemen t	Malware Re engineering	Application Vulnerability Testing	Security Assurance	Secure SDLC Training
Platforms / Systems	Security Patch Management	Antivirus/Anti -Malware Management	Endpoint Security	Data Loss Prevention	Encryption	Professional cybercrime	Malware Engineering	
EUC, Mobility & Cloud	Communicatio n Interception	Network Security	Antivirus/Anti -Malware Management	MDM / device Loss and Theft	Application Security Assurance	SIP Vulnerabilitie s protection	Penetration & Vulnerability Testing	IP phone & PBX protection

Full Security Protection

Standart and Framework



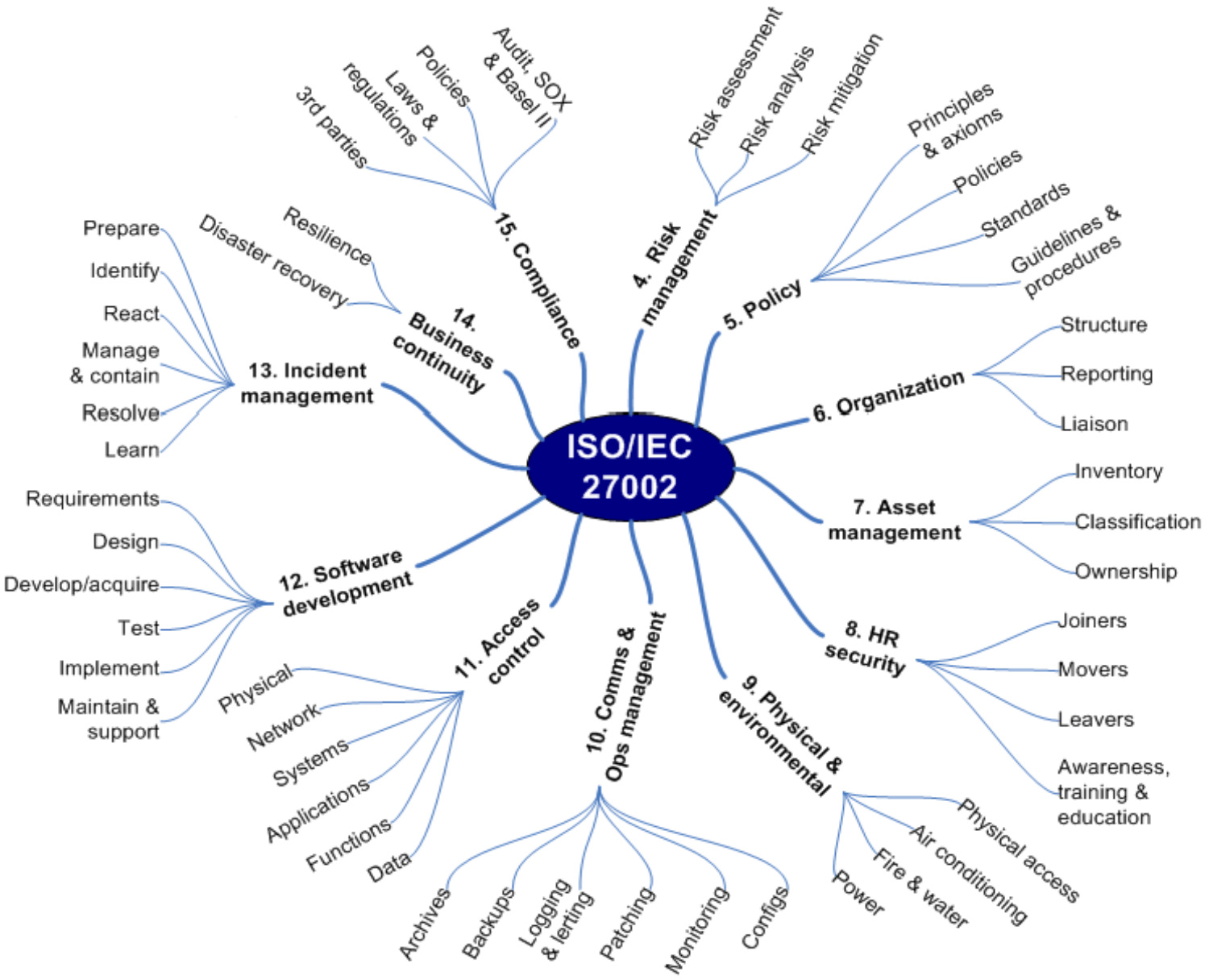
Cobit 5 (ISACA, 2012)



TOGAF


Preliminary
A.
Architecture
Vision
B.
Business
Architecture
C.
Information
Systems
Architectures
D.
Technology
Architecture
E.
Opportunities
and
Solutions
F.
Migration
Planning
G.
Implementation
Governance
H.
Architecture
Change
Management
Requirements
Management
© The Open Group

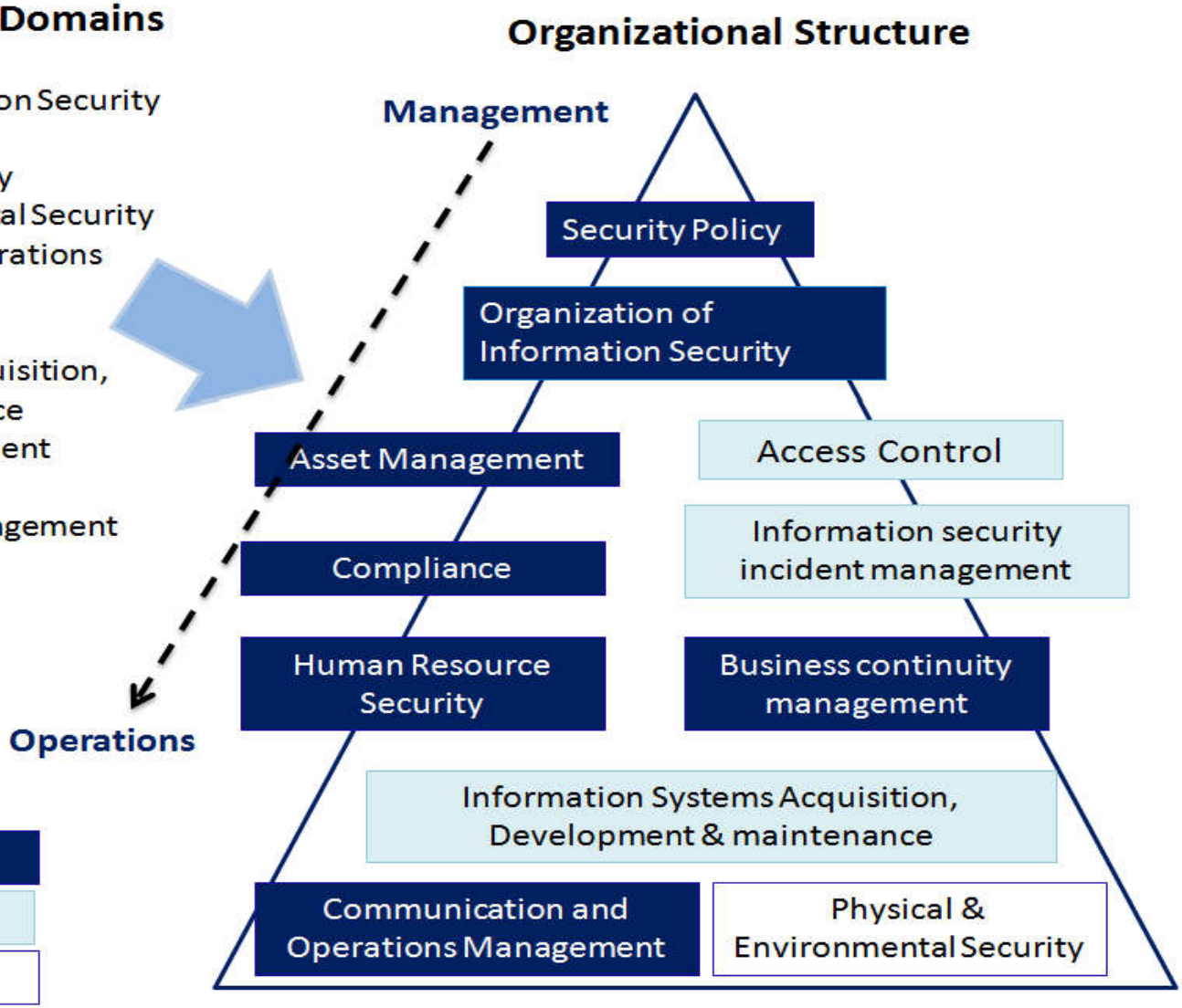
Peta Tata Kelola SMKI



Aspek Tata Kelola SMKI

The 11 ISO/IEC 27001 Domains

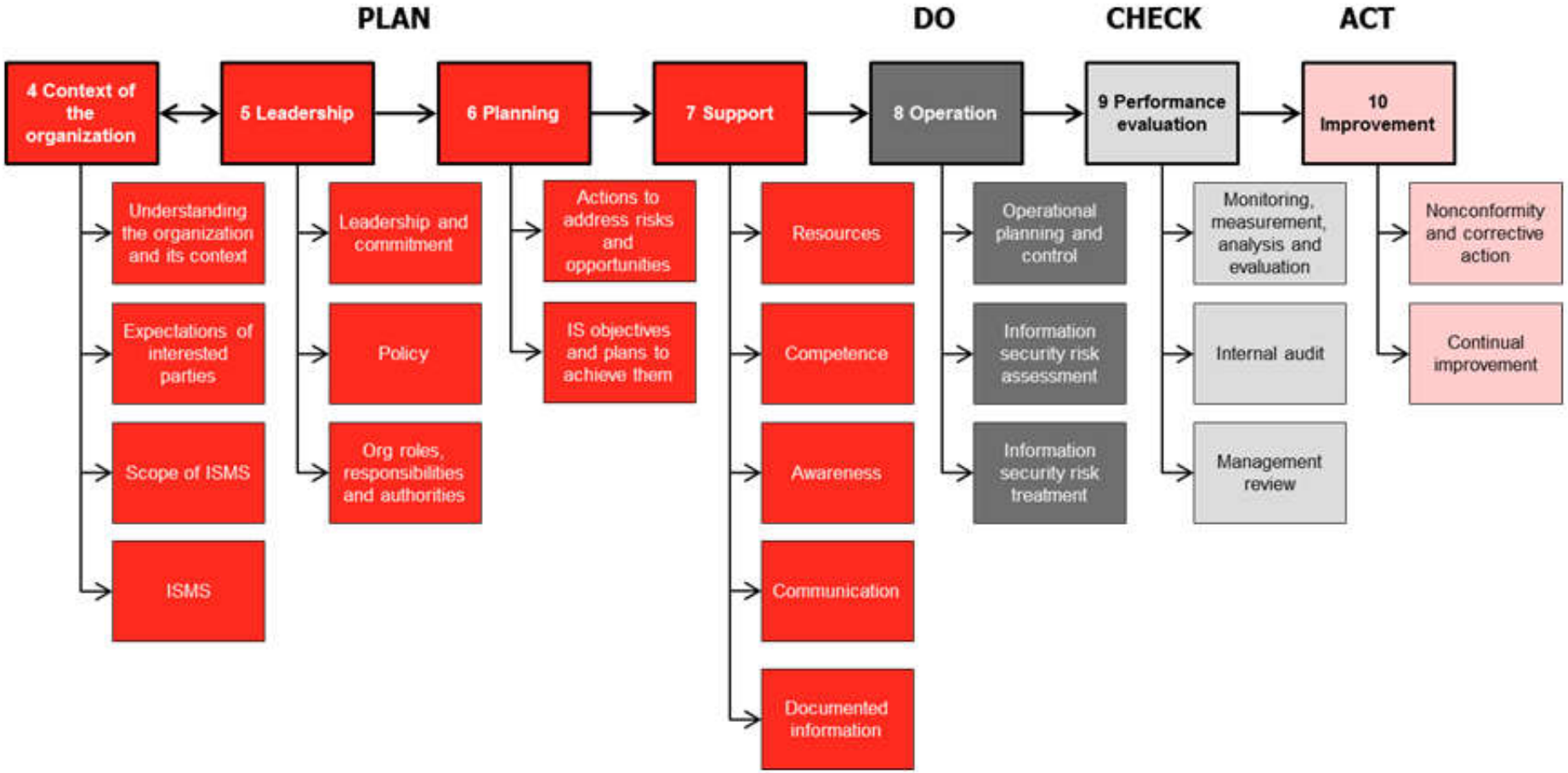
- ❑ Security Policy
- ❑ Organization of Information Security
- ❑ Asset Management
- ❑ Human Resources Security
- ❑ Physical and Environmental Security
- ❑ Communications and operations management
- ❑ Access control
- ❑ Information Systems Acquisition, Development & maintenance
- ❑ Information security incident management
- ❑ Business Continuity Management
- ❑ Compliance



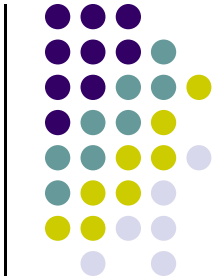
Legend:

- Management Aspect
- Technical Aspect
- Physical Aspect

Konsep PDAC


PLAN
DO
CHECK
ACT
4 Context of the organization
5 Leadership
6 Planning
7 Support
8 Operation
9 Performance evaluation
10 Improvement
Understanding the organization and its context
Expectations of interested parties
Scope of ISMS
ISMS
Leadership and commitment
Policy
Org roles, responsibilities and authorities
Actions to address risks and opportunities
IS objectives and plans to achieve them
Resources
Competence
Awareness
Communication
Documented information
Operational planning and control
Information security risk assessment
Information security risk treatment
Monitoring, measurement, analysis and evaluation
Internal audit
Management review
Nonconformity and corrective action
Continual improvement

INDEKS KAMI



Information Security Indexs (INDEXS KAMI)

(Bridging Test to compliance SNI ISO IEC 27001)

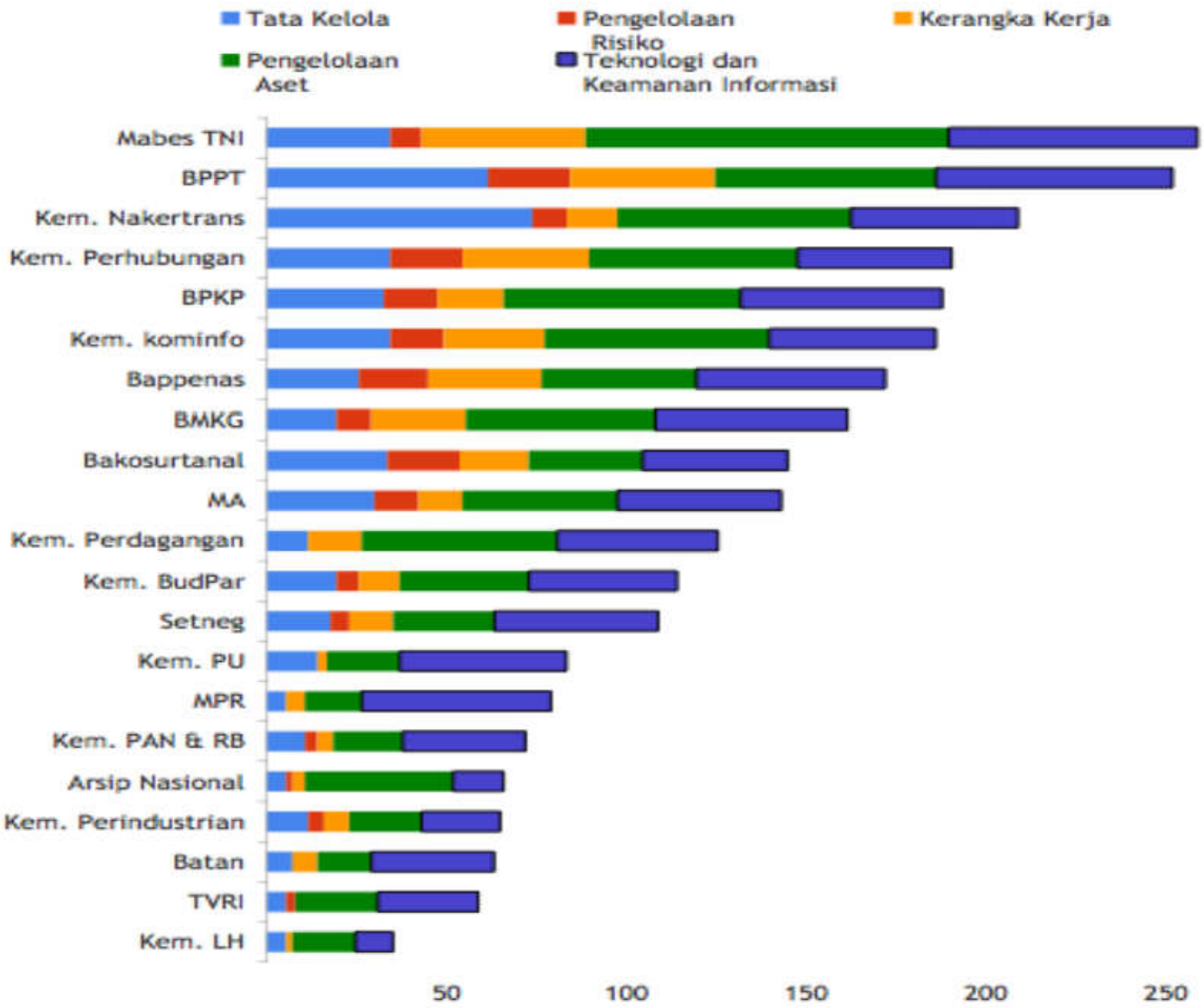
NO	Index
1	Governance
2	Risk Management
3	Framework
4	Asset Management
5	Technology & Information Security

Information Security Indexs/Indeks KAMI was initiated in 2007 especially for central government in implementing information security government ranks

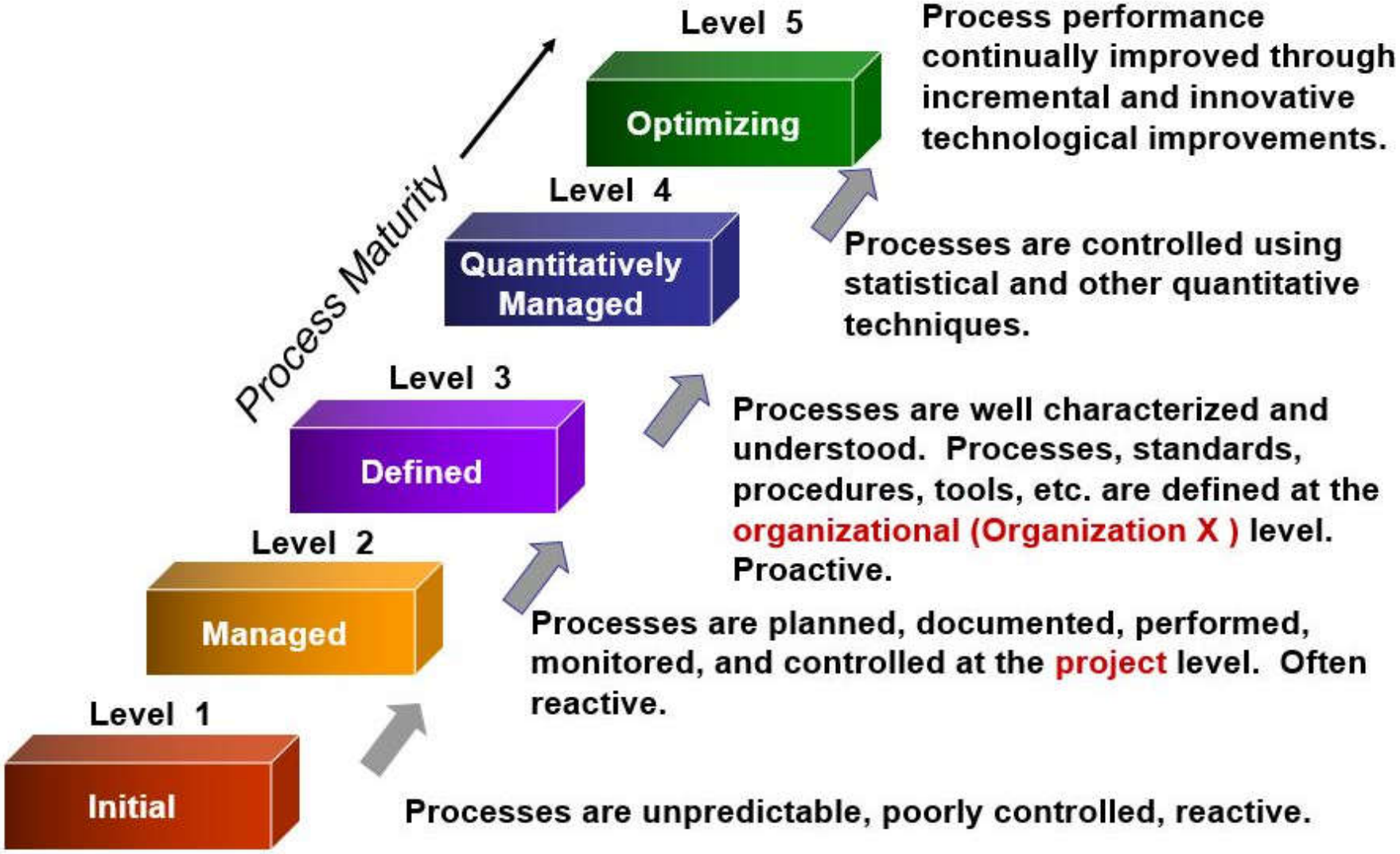
SNI ISO/IEC 27001:2009 Information Security Management System

1	Information Security Policy
2	Organisation of Information Security
3	Asset Management
4	Human Resources Security
5	Physical and Environmental Security
6	Communications and Operations Management
7	Access Control
8	Information systems acquisition, development and maintenance
9	Information security incident management
10	Business Continuity Management
11	Compliance

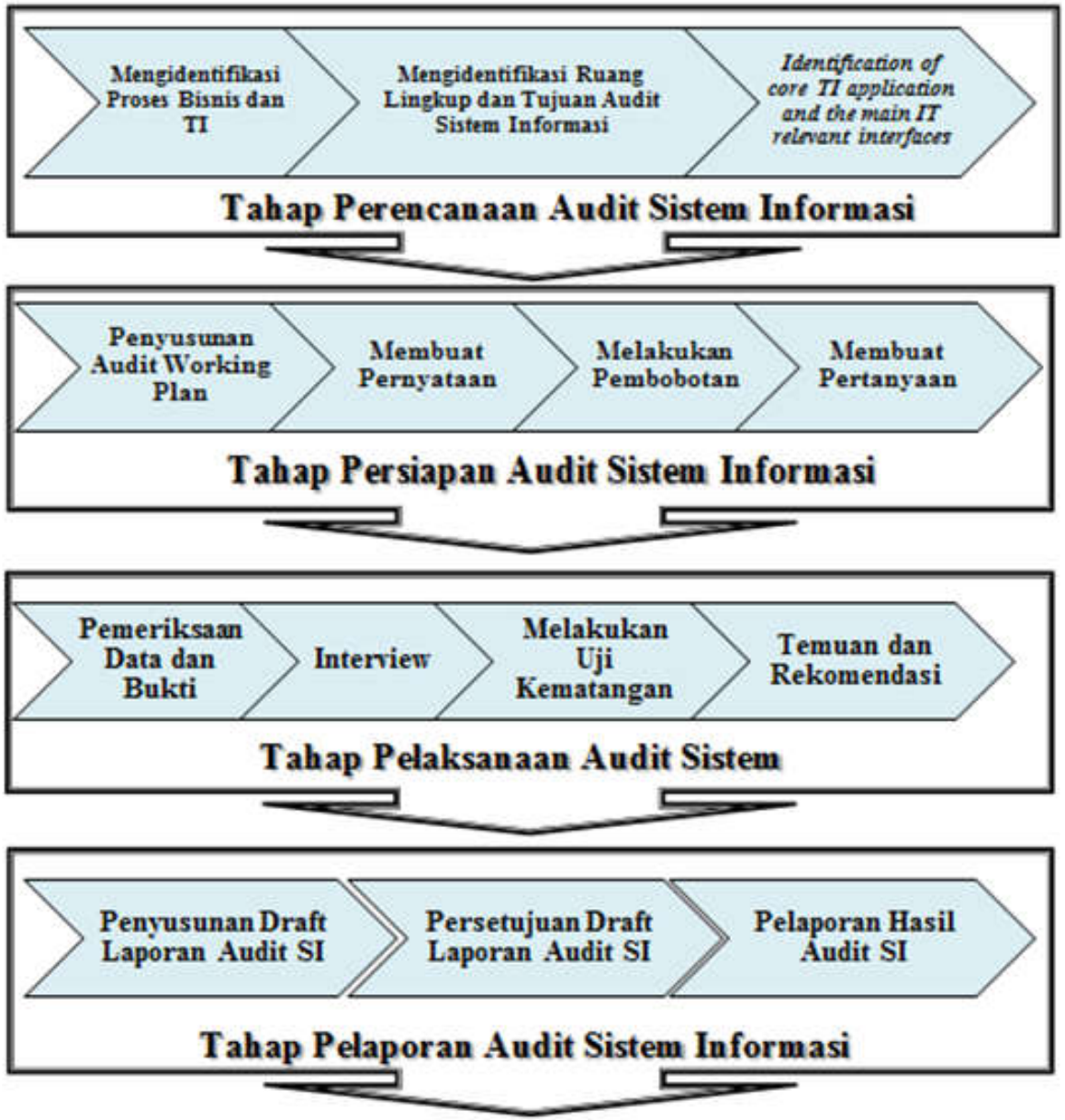
Peringkat Indeks KAMI 2011



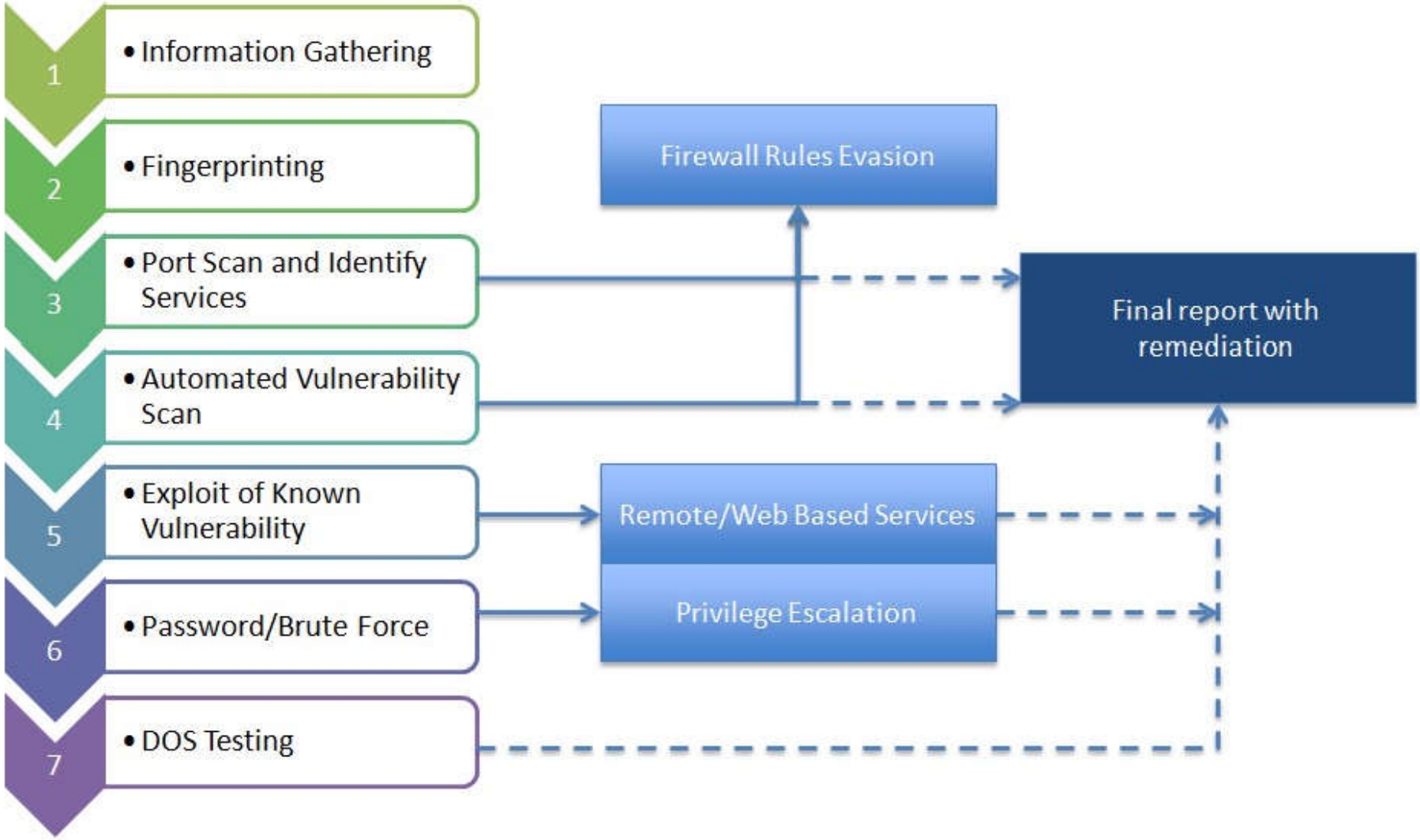
Tingkat Kematangan (CMMI)



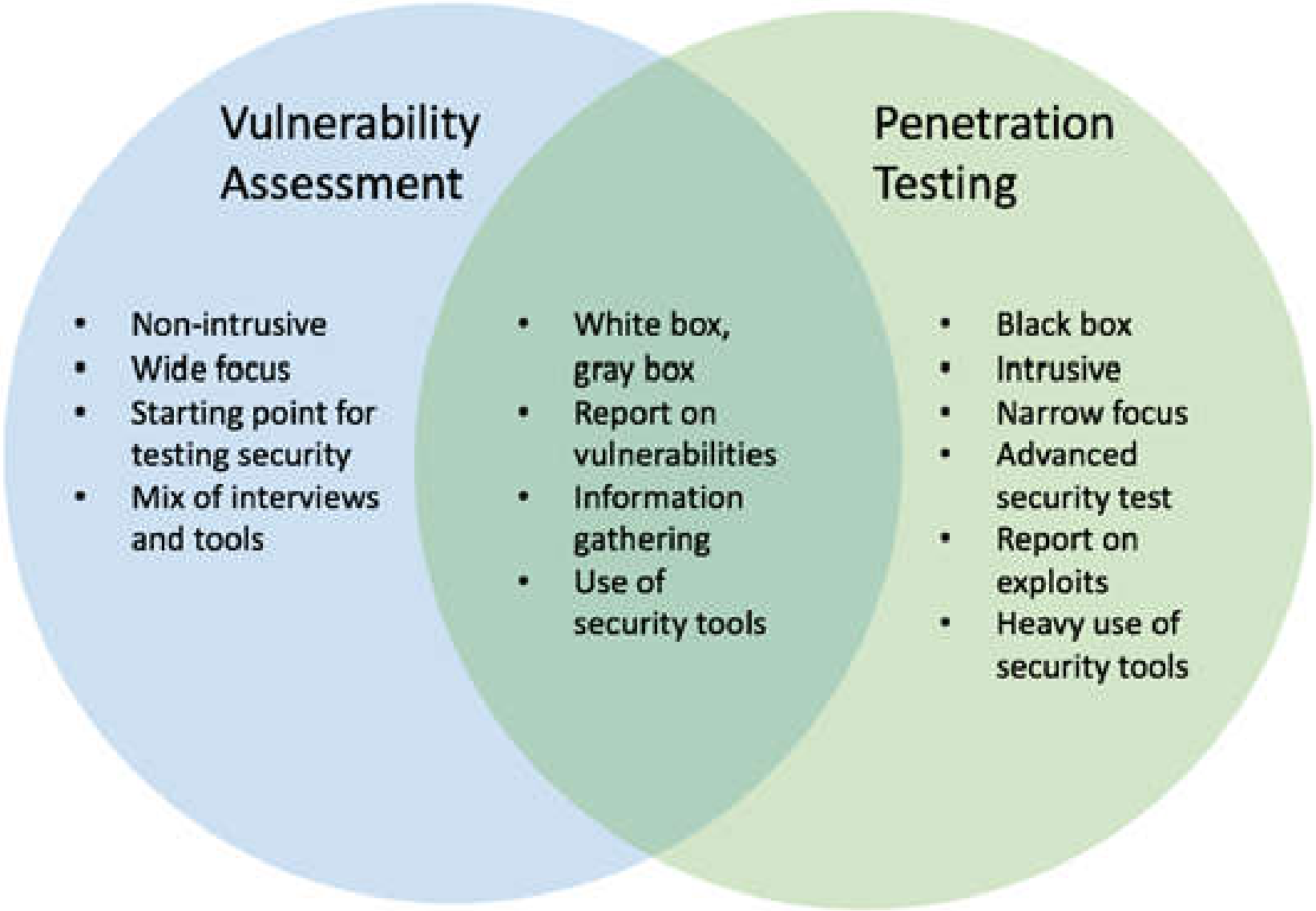
Tahapan Audit Sistem Informasi



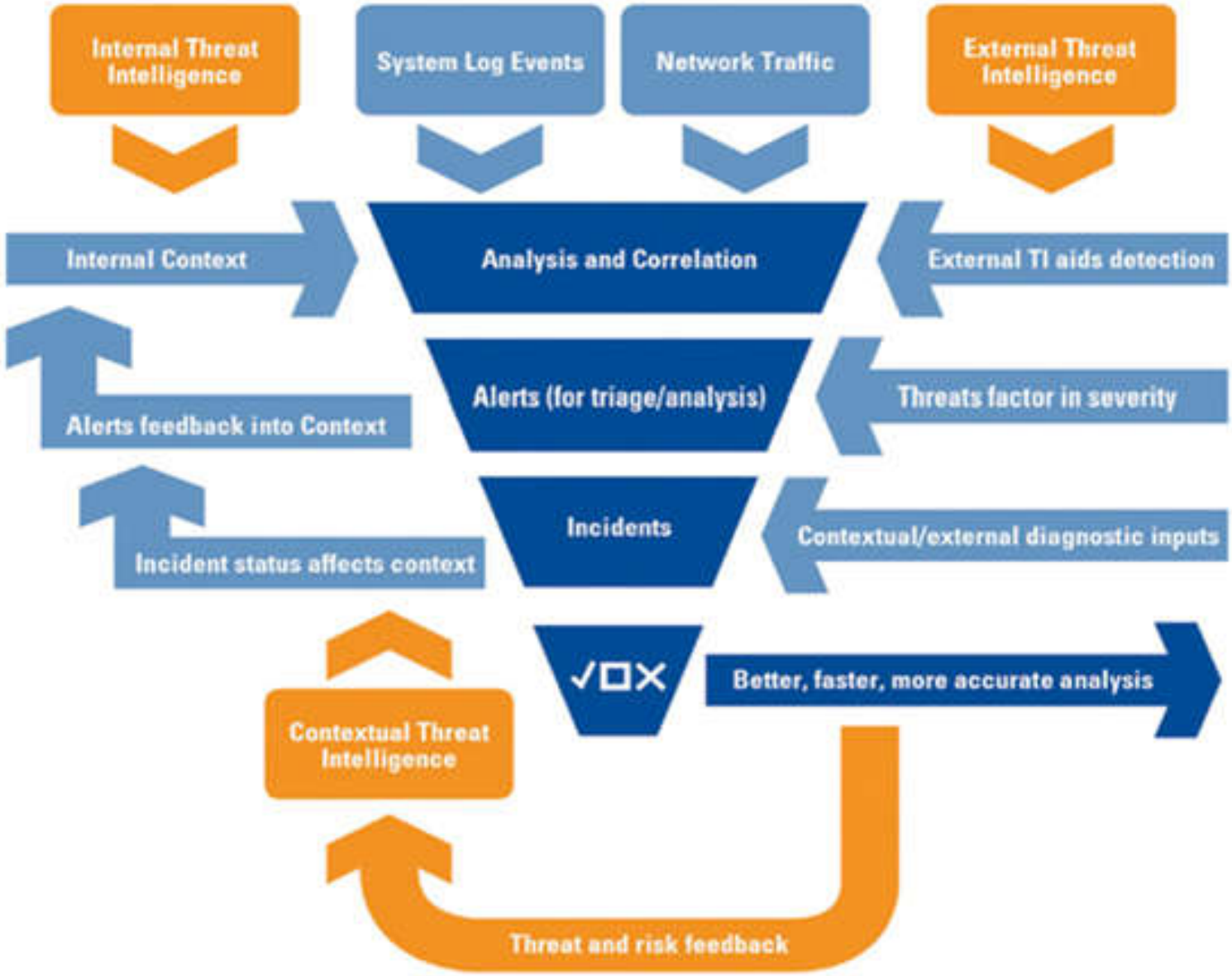
Tahapan Security Assessment



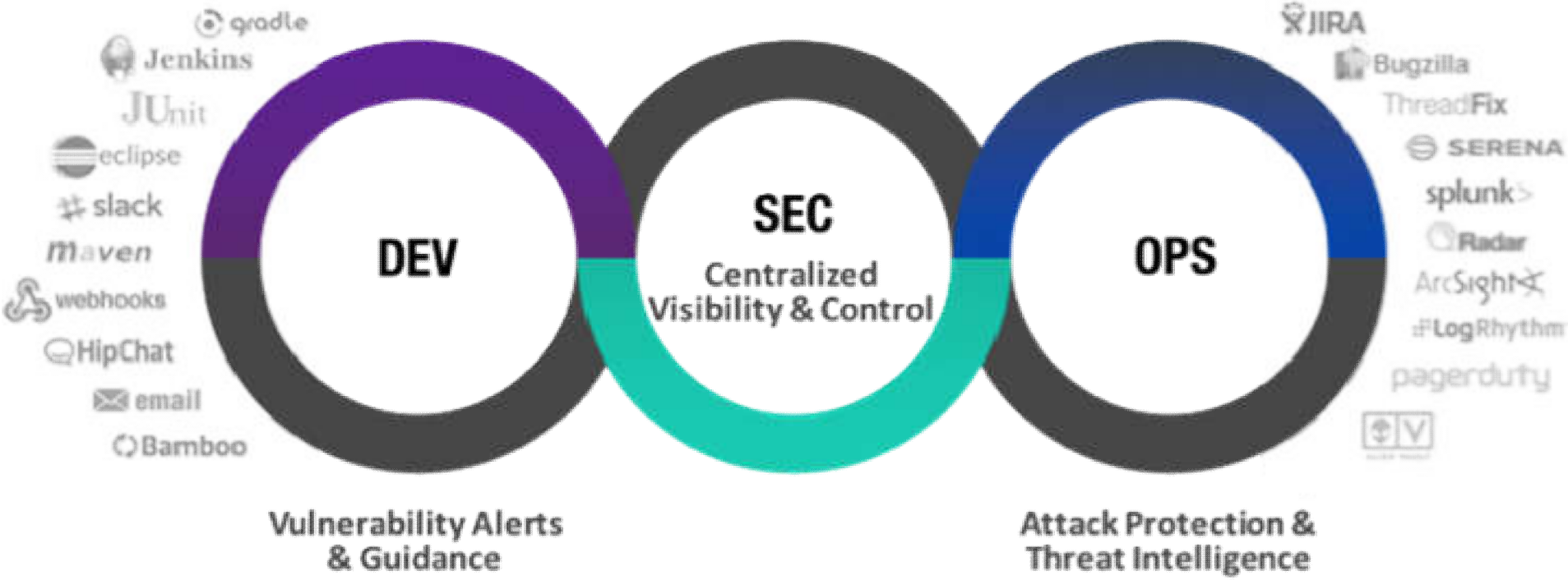
Vulnerability vs Pentest



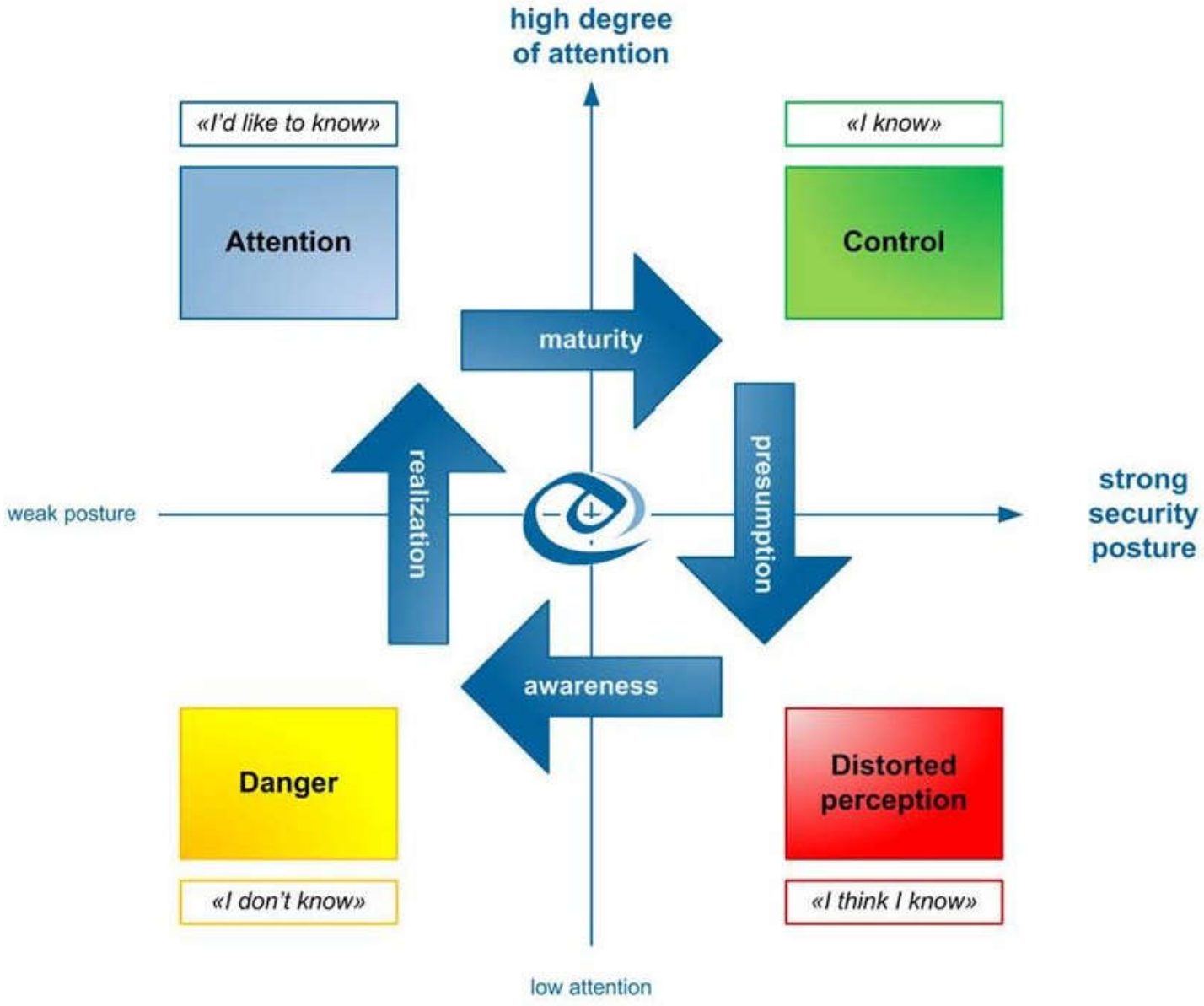
Security Monitoring



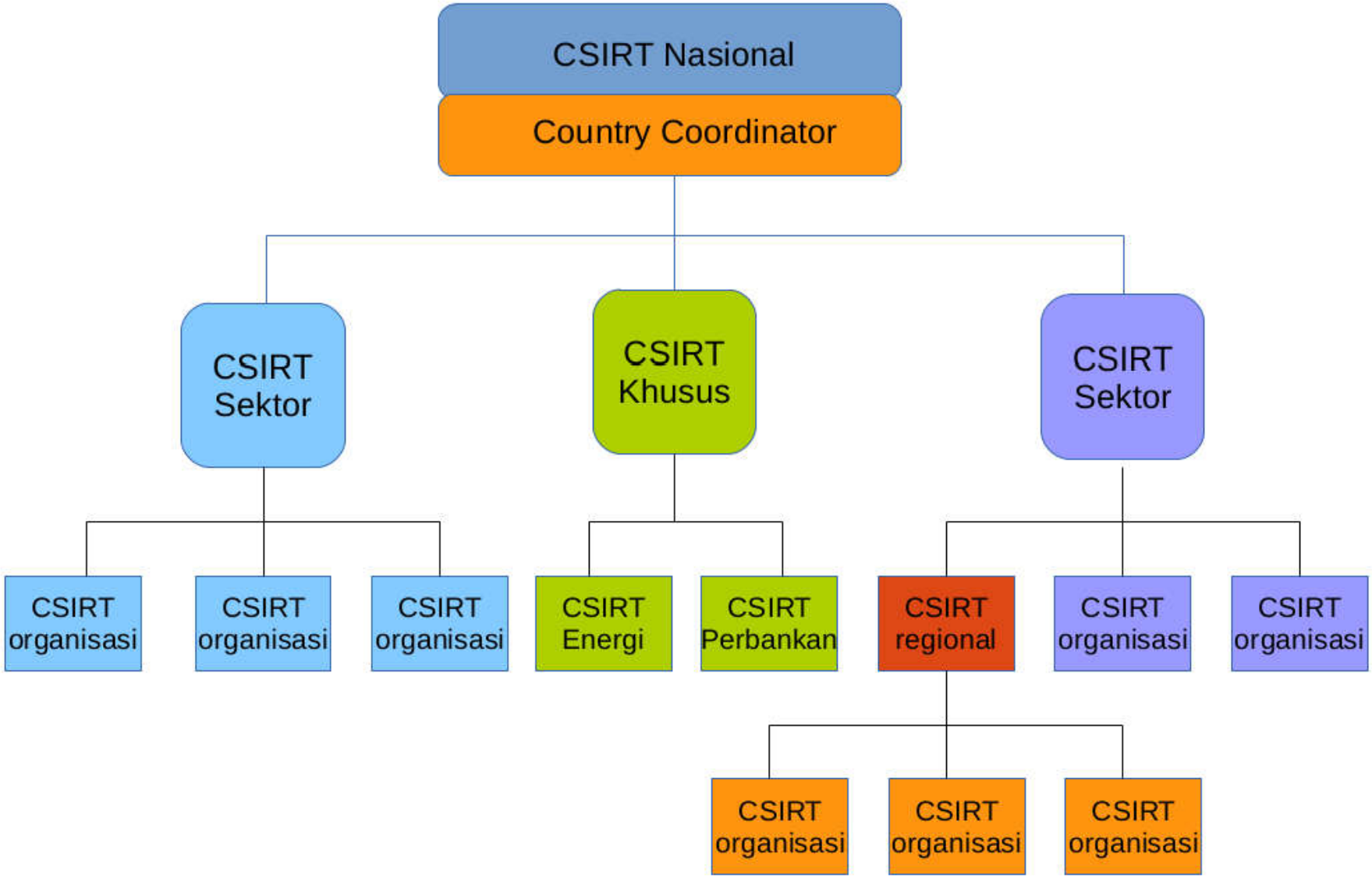
Dev Sec Ops


gradle
Jenkins
JUnit
eclipse
slack
Maven
webhooks
HipChat
email
Bamboo
DEV
SEC
Centralized
Visibility & Control
OPS
JIRA
Bugzilla
ThreadFix
SERENA
splunk>
Radar
ArcSight
LogRhythm
pagerduty
Vulnerability Alerts
& Guidance
Attack Protection &
Threat Intelligence

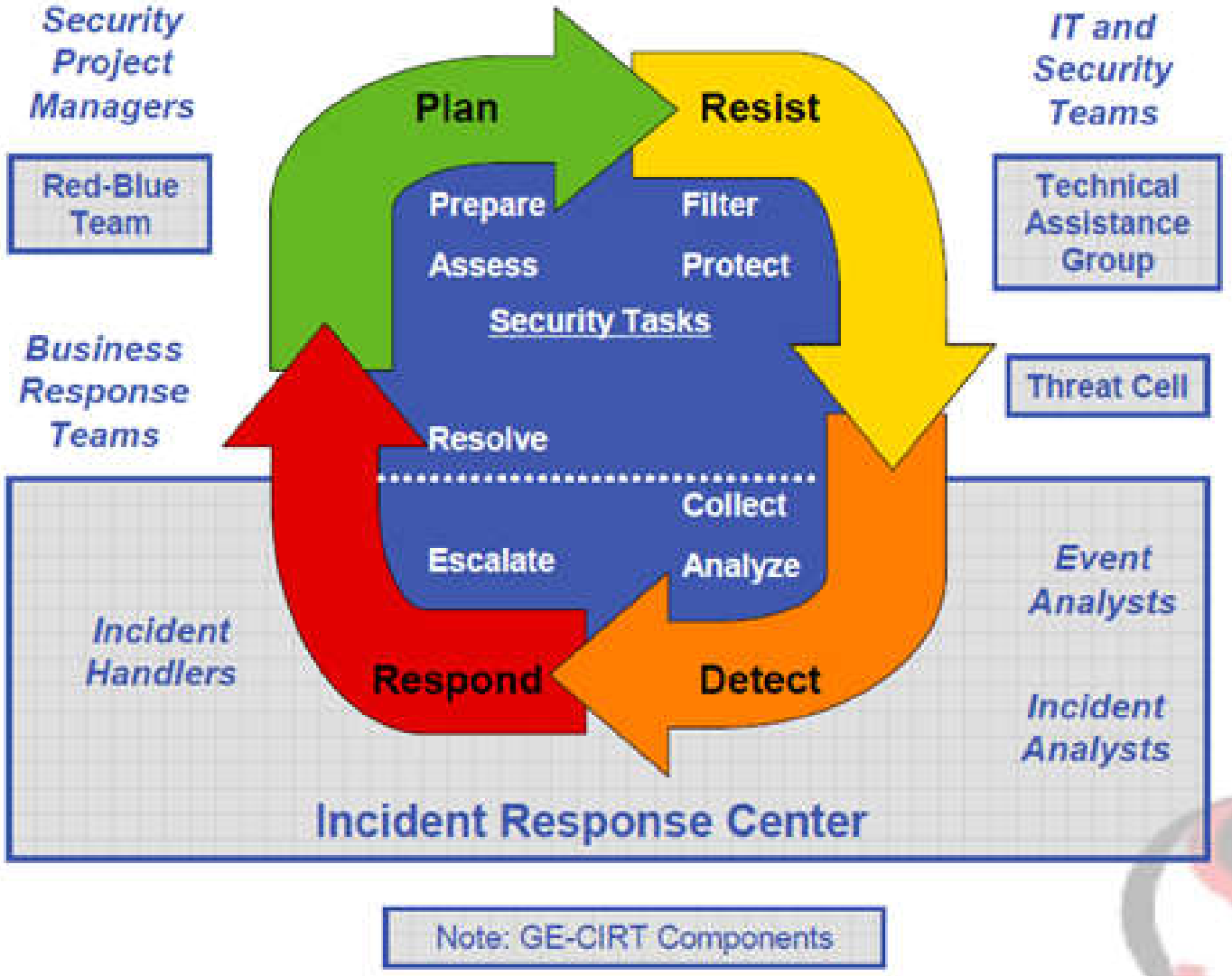
From Awareness to Security



Struktur Organisasi CSIRT

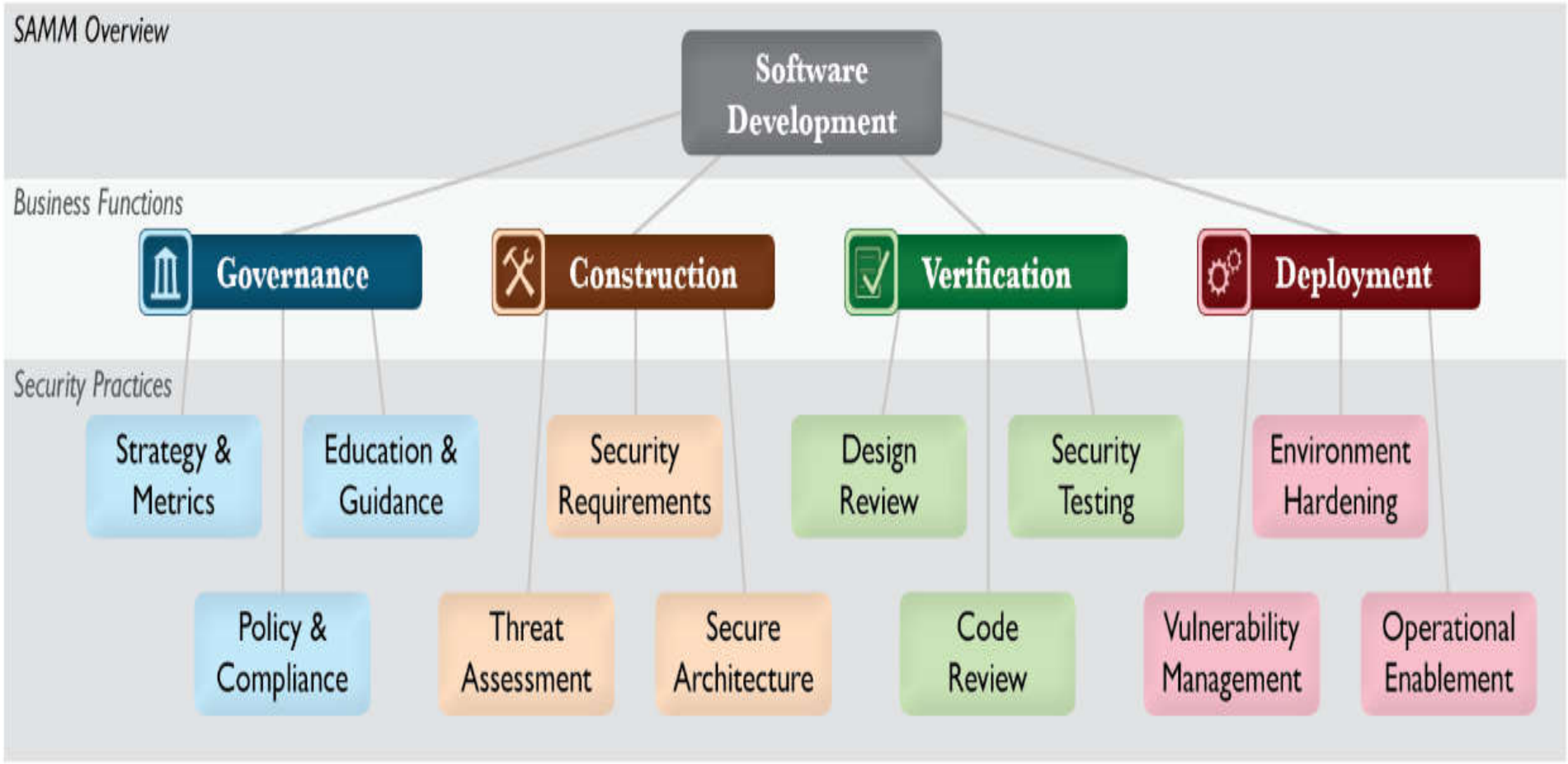


Siklus CSIRT

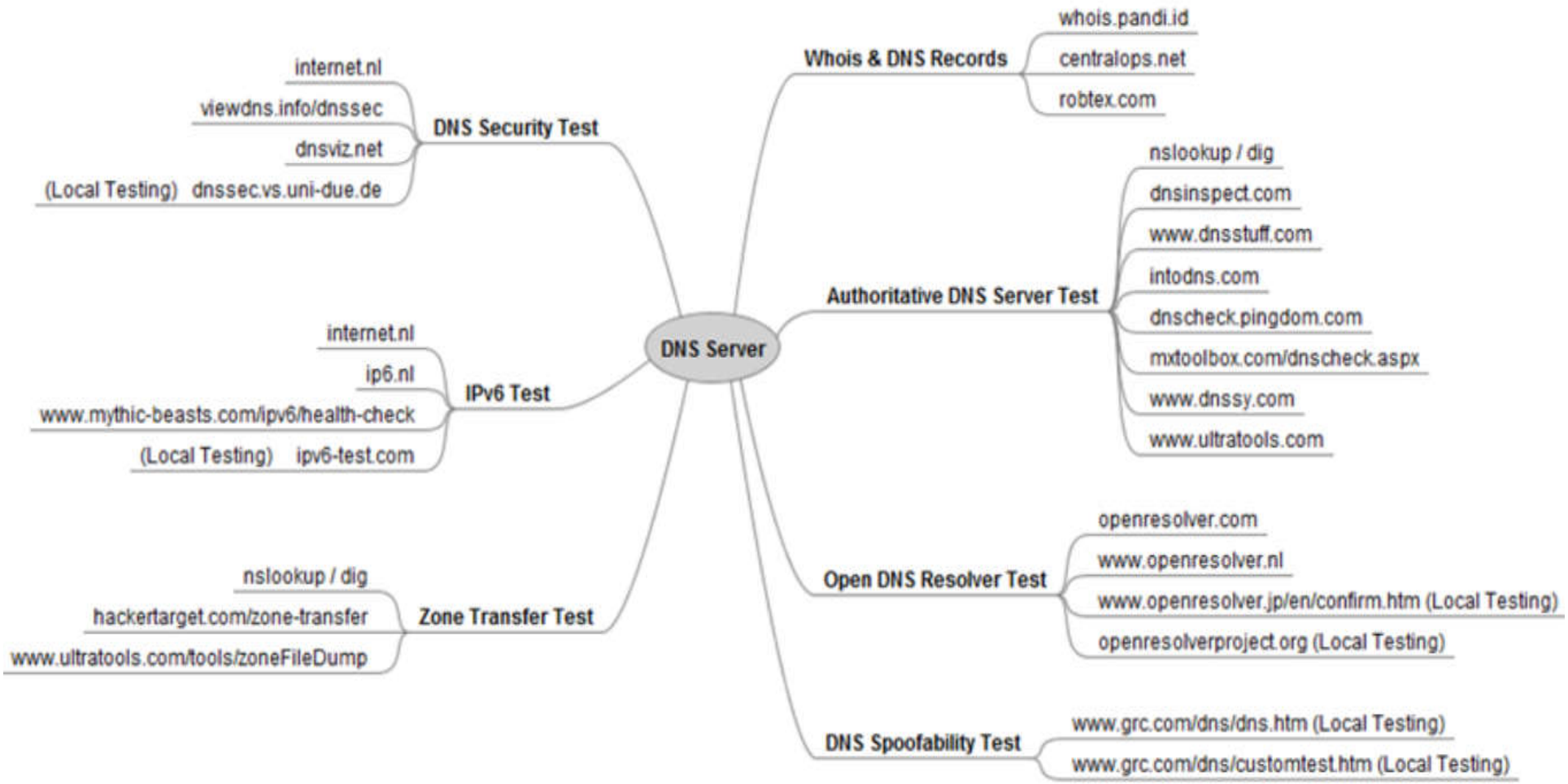


Source: Richard Bejtlich, *CIRT-Level Response to Advanced Persistent Threat*

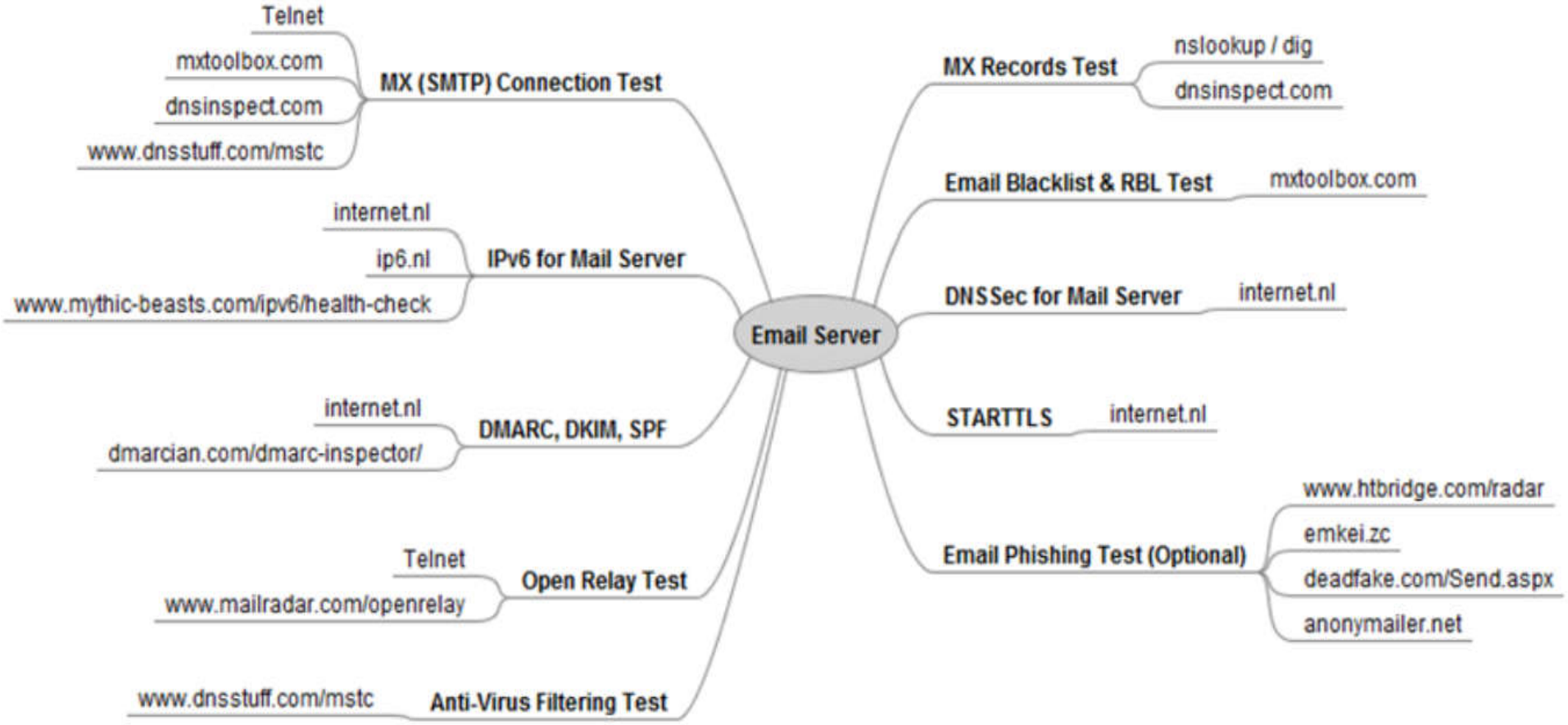
Secure Coding (SDLC)



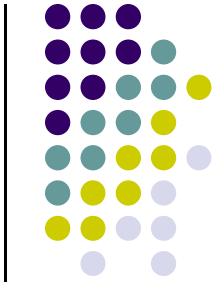
Test DNS Server

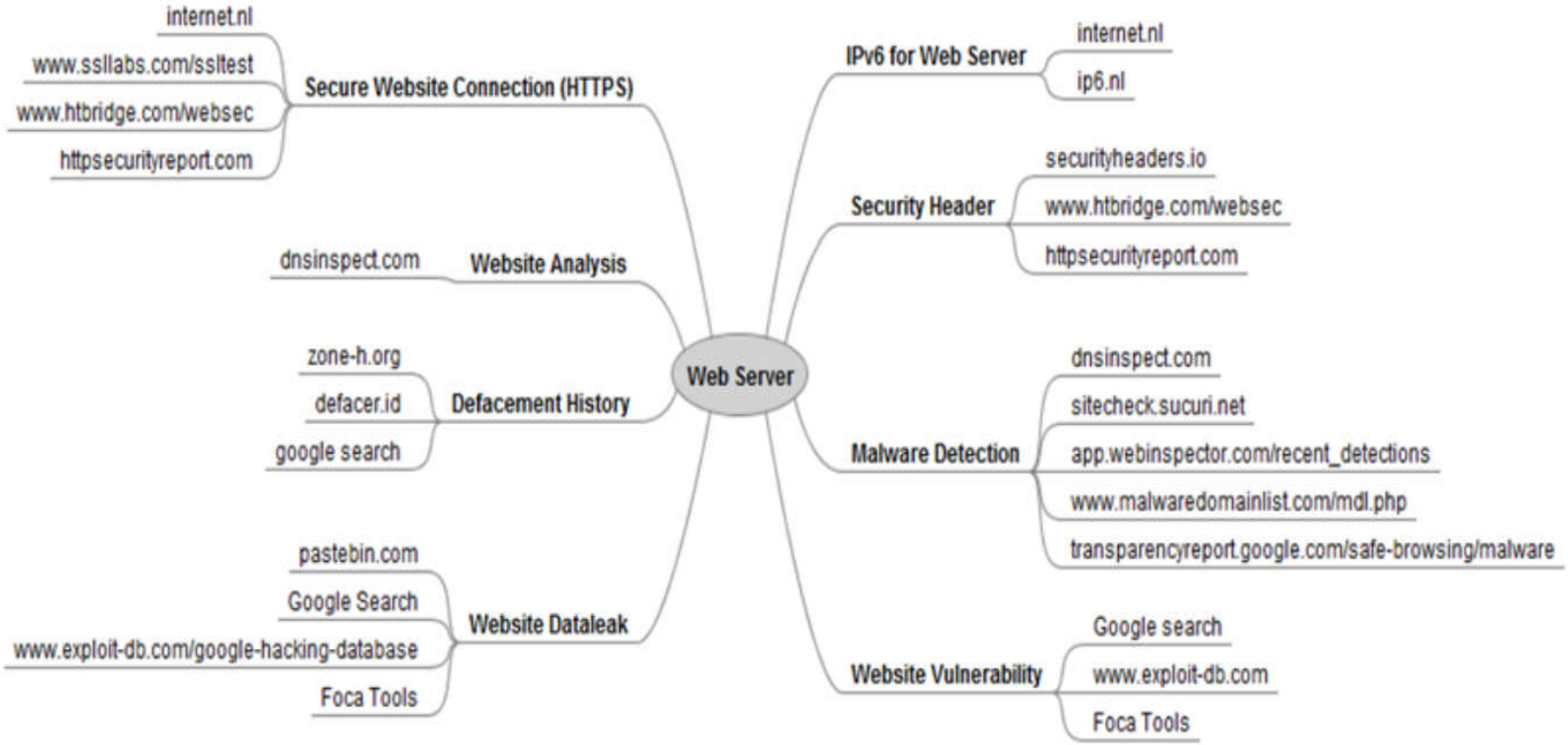


Test Email Server

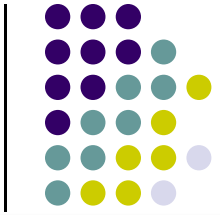


Test Web Server





Indek KIDI (1)



No.	KEMENTERIAN	ASSESSMENT				Rata-Rata
		DNS Server	Email Server	Web Server & Apps.	Info. Gathering	
1.	Kementerian Koordinator Bidang Politik, Hukum, dan Keamanan	9.50	10.00	5.75	9.20	8.61
2.	Kementerian Koordinator Bidang Perekonomian	9.50	10.00	5.30	8.80	8.40
3.	Kementerian Badan Usaha Milik Negara	9.25	9.20	5.05	9.60	8.28
4.	Kementerian Komunikasi dan Informatika	10.00	9.00	4.65	9.33	8.25
5.	Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi	9.25	8.80	5.20	9.60	8.21
6.	Kementerian Pertahanan	9.50	8.40	5.25	8.80	7.99
7.	Kementerian Riset, Teknologi, dan Pendidikan Tinggi	9.50	8.40	5.75	8.20	7.96
8.	Kementerian Koordinator Bidang Kemaritiman	9.50	9.60	3.00	9.60	7.93
9.	Kementerian Koordinator Bidang Pembangunan Manusia dan Kebudayaan	8.50	8.40	5.50	8.80	7.80
10.	Kementerian Hukum dan Hak Asasi Manusia	9.50	10.00	2.50	9.20	7.80
11.	Kementerian Agama	8.50	9.60	5.25	7.60	7.74
12.	Kementerian Koperasi dan Usaha Kecil dan Menengah	8.00	7.60	4.75	9.60	7.49
13.	Kementerian Pariwisata	8.25	8.00	4.00	9.60	7.46
14.	Kementerian Luar Negeri	8.50	8.80	3.75	8.80	7.46
15.	Kementerian Pemuda dan Olahraga	9.00	8.40	3.25	9.20	7.46
16.	Kementerian Lingkungan Hidup dan Kehutanan	7.50	9.00	4.00	9.00	7.38
17.	Kementerian Energi dan Sumber Daya Mineral	7.75	9.60	4.65	7.40	7.35
18.	Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi	7.75	8.00	4.00	9.60	7.34
19.	Kementerian Ketenagakerjaan	8.50	8.40	2.75	9.60	7.31
20.	Kementerian Sekretariat Negara	8.25	7.20	4.06	9.60	7.28

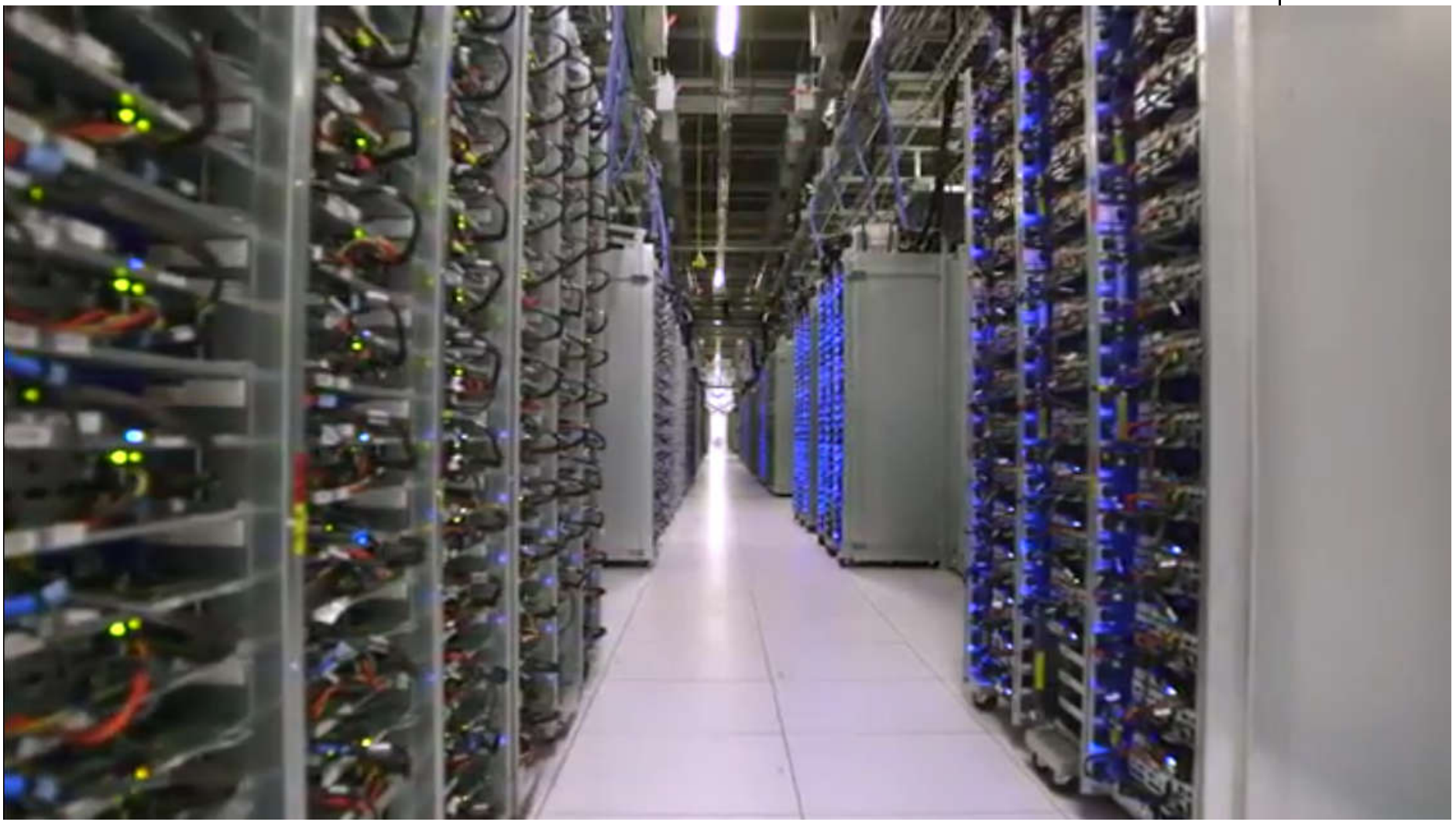
Indek KIDI (2)

21.	Kementerian Keuangan	8.50	8.00	4.30	8.00	7.20
22.	Kementerian Pendidikan dan Kebudayaan	6.75	8.80	5.20	8.00	7.19
23.	Kementerian Agraria dan Tata Ruang (BPN)	8.00	7.60	5.25	7.80	7.16
24.	Kementerian Sosial	8.50	8.00	3.75	8.40	7.16
25.	Kementerian Pertanian	9.25	8.80	4.95	5.40	7.10
26.	Kementerian Perdagangan	10.00	7.60	3.50	7.20	7.08
27.	Kementerian Kesehatan	5.50	10.00	3.75	8.80	7.01
28.	Kementerian Kelautan dan Perikanan	9.50	9.20	2.75	6.20	6.91
29.	Kementerian Pemberdayaan Perempuan dan Perlindungan Anak	8.25	8.00	4.00	7.20	6.86
30.	Kementerian Perencanaan Pembangunan Nasional	5.25	8.20	5.00	8.80	6.81
31.	Kementerian Perhubungan	7.75	6.80	5.80	6.60	6.74
32.	Kementerian Dalam Negeri	6.75	8.40	3.00	8.80	6.74
33.	Kementerian Perindustrian	9.00	5.60	3.25	8.80	6.66
34.	Kementerian Pekerjaan Umum dan Perumahan Rakyat	6.75	8.60	2.95	7.40	6.43

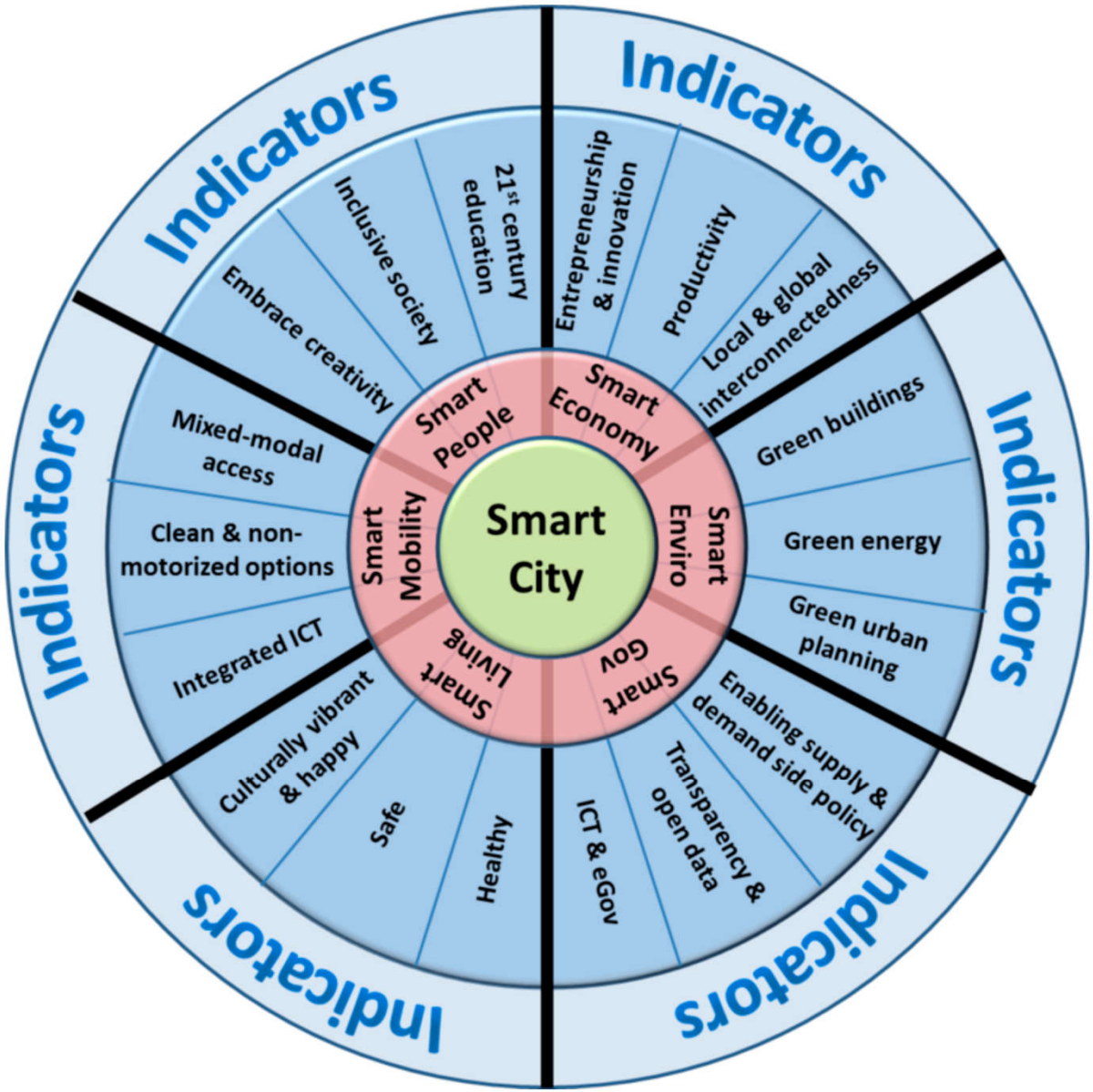
Keterangan :

Level Keamanan	Angka	Warna
Sangat Aman	9 – 10	
Aman	7 – 8.99	
Sedang	5 – 6.99	
Rentan	3 – 4.99	
Sangat Rentan	0 – 2.99	

Google Datacenter



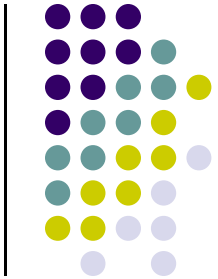
Dimensi Smart City



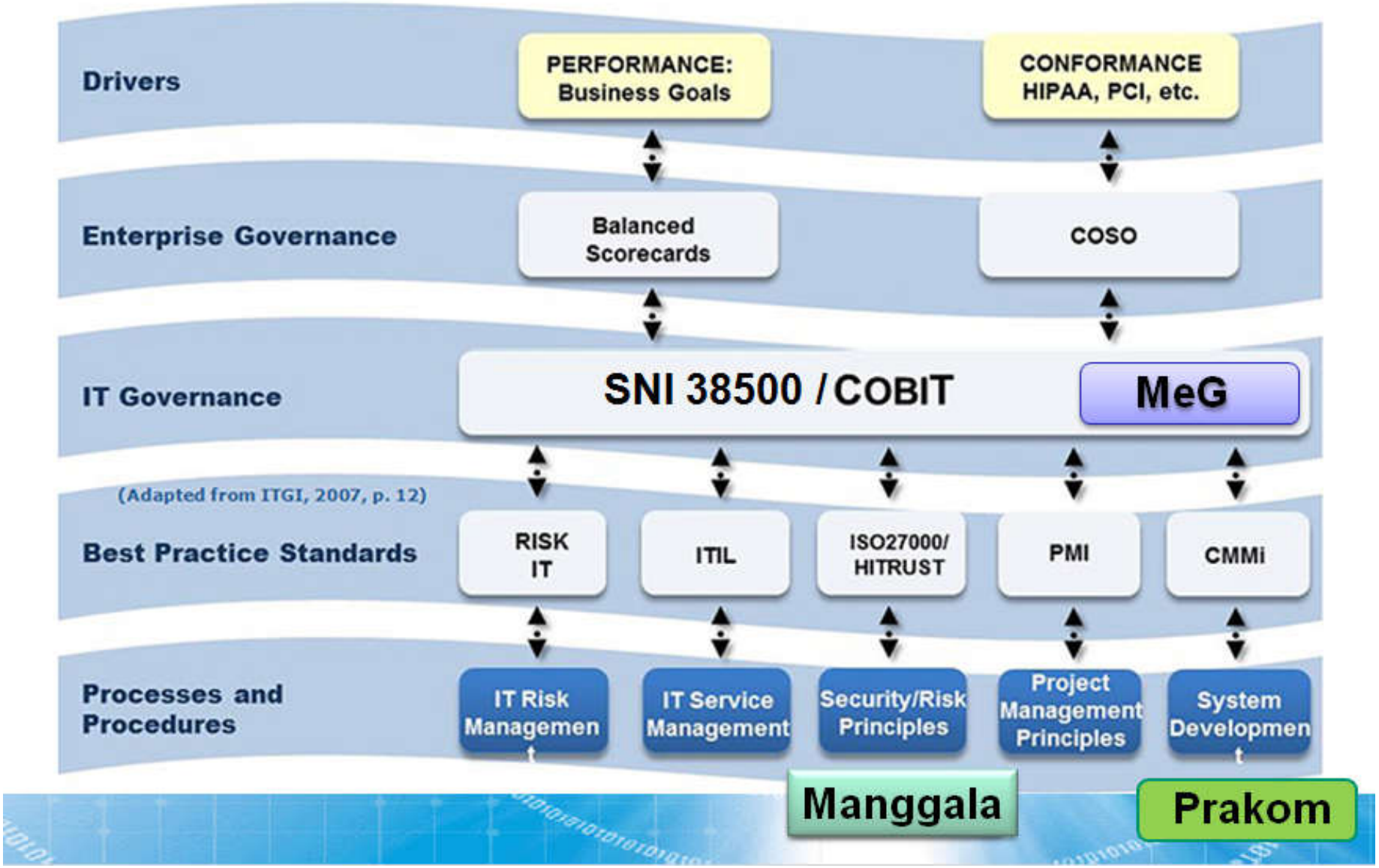
Fungsi CIO


CREATE VALUE
IT Sourcing Management
IT Program Management
IT Delivery Management
MANAGE VALUE
IT Value Management
IT M&A Management
IT Architecture Management
IT Value Business
CIO
IT Value Governance
IT Resource Management
IT Risk & Security Management
IT Innovation Management
IT Operations Management
IT Strategy Planning Management
IT Customer Relationship Management
REALIZE VALUE
IT Eco-System Management

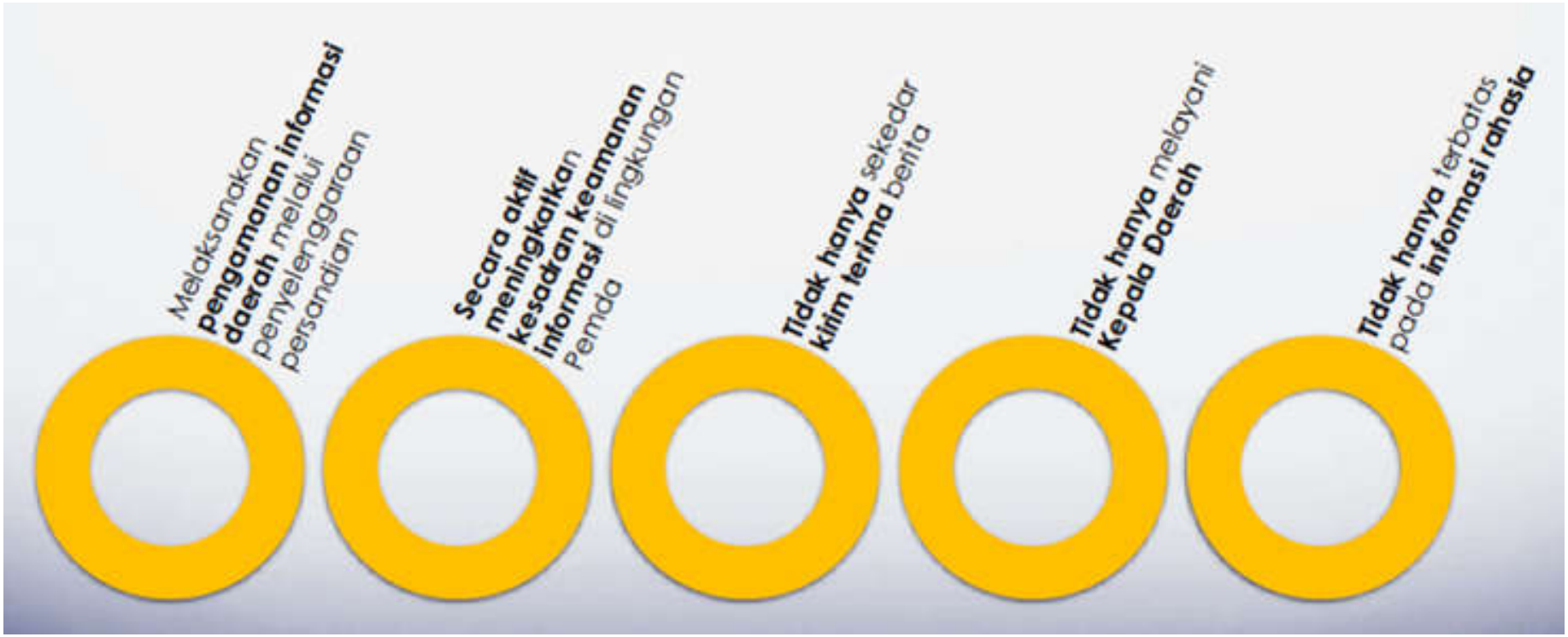
Government CIO



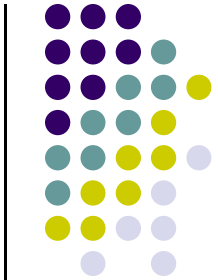
Tata Kelola Sistem Elektronik



Paradigma Baru Persandian



Regulasi Bidang Persandian



- UU No23 Th2014 (Pemerintah Daerah)
- PP No18 Th2016 (Perangkat Daerah)
- Permenkominfo No14 Th2016 (Nomenklatur)
- Perbup Pati No47 Th2016 (Tupoksi Dinkominfo)
- Perka Lemsaneg No7 Th2017 (Persandian)
- Perpres No53 Th2017 (Badan Siber Sandi Neg)
- Permenkominfo No26 Th2007 (ID-SIRTII)
- Permenkominfo No41 Th2007 (TataKelola TIK)
- Permenkominfo No4 Th2016 (SMPI)

Sumber Referensi (1)

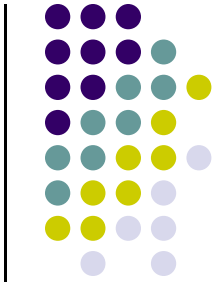
- http://www.youtube.com/watch?v=HQIG_vMGe1A
  (Getting Started With Digital Modes)

- https://www.youtube.com/watch?v=WRv9DbqnnDg
  (WinLink Digital Mode)

- https://www.youtube.com/watch?v=dxIOtn0Bsnc
  (D-STAR and the Icom RS-MS1A Android)

- https://www.youtube.com/watch?v=XZmGGAbHqa0
  (Inside Google Data Center)

Sumber Referensi (2)



- http://jdih.lemsaneg.go.id/wp-content/uploads/2017/06/Perka-Lemsaneg-No-7-tahun-2017-ttg-GarsanSigned.pdf

  (Perka Lemsaneg No 7 Tahun 2017 Tentang Pedoman Pengamanan Informasi di Lingkungan Pemerintah Daerah Provinsi dan Kabupaten / Kota)

- http://birohukum.jogjaprov.go.id/storage/1476087788pergub31-2016.pdf

  (Pergub DIY No 31 Tahun 2016 Tentang Sistem Manajemen Keamanan Informasi)

Terima Kasih

“There is No Security Patch for Human Stupidity”

Downloads

https://goo.gl/8EFddd

Telegram - Cyber Security Pati

https://t.me/joinchat/CcDMSk3uwDOOkgnBx66y9w