z/OS mainframe

Security Business Value

Agenda

1. Korte persoonlijke introductie
2. Positionering z/OS mainframe security
3. Maturity, governance & risks in samenhang

whoami

- Mainframe ervaring sinds 1978

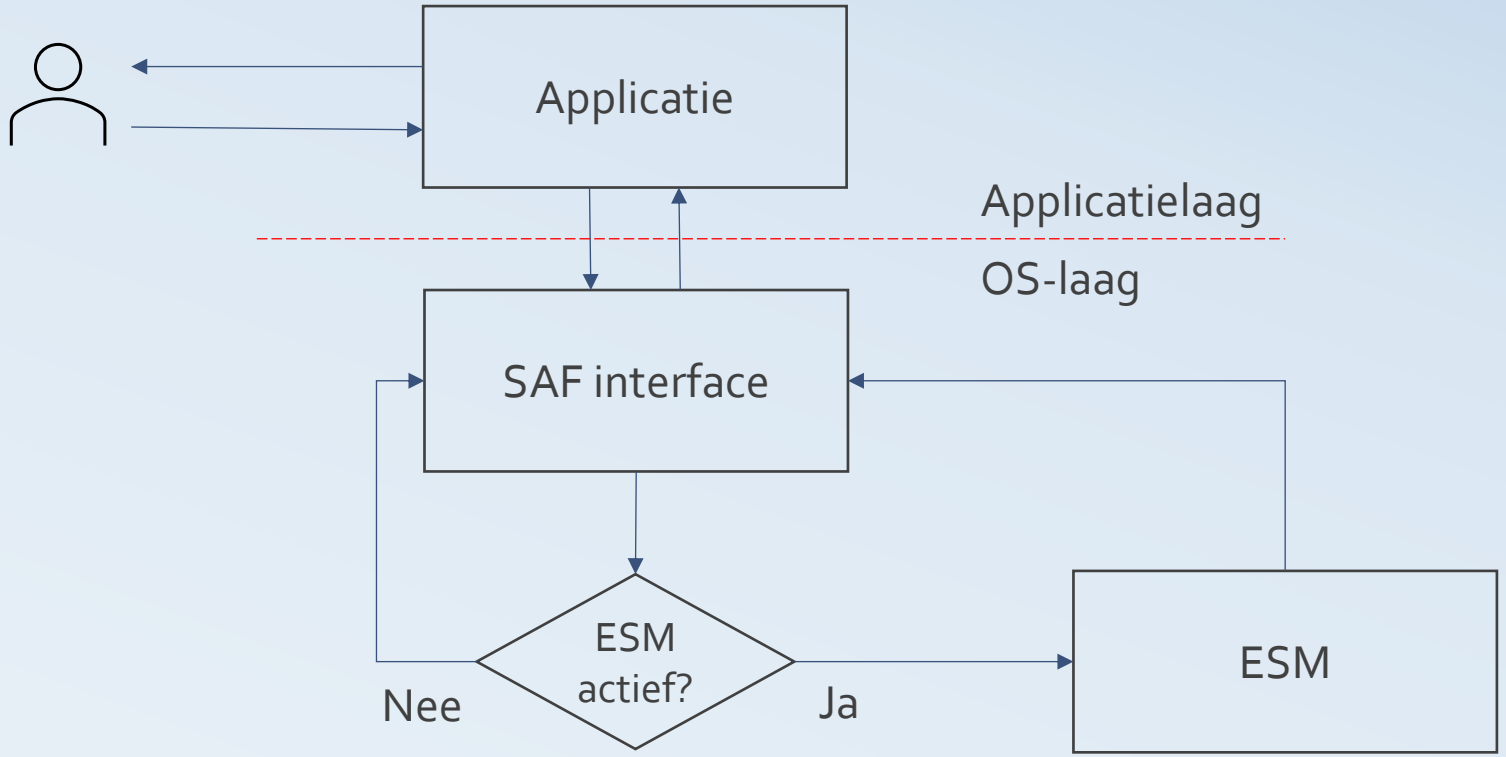
- RACF ervaring sinds 1992
  - Admin ⇨ Impl. tech lead ⇨ Auditor
- ISO 27K1 ISMS implementaties sinds 2015
- C-letter soep sinds 2001
- Conference speaker
  - Guide Share Europe
  - ISACA
  - EC-Council
  - Vanguard Integrity Professionals
- Maar vooral…

Positionering z/OS mainframe security

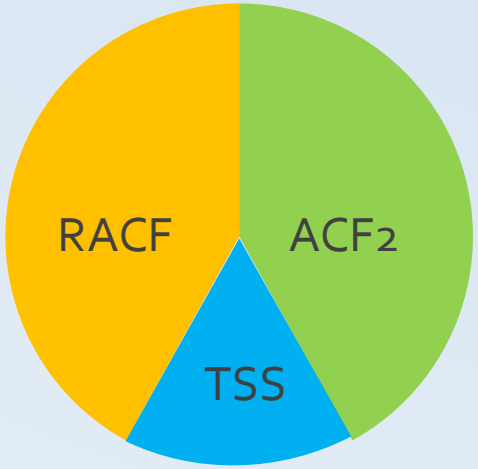
z/OS vs IX/UX/Windows

Eigenschap	z/OS Mainframe	IX/UX/Windows server
Security integratie	Integratie in architectuur	Security als add-on
Security architectuur	Centraal, fijnmazig	Decentraal, afhankelijk van configuratie
Gebruikersmodel	Centraal via SAF / ESM	Lokale users + LDAP / AD
Toegangscontrole	Per resource	Bestandsniveau + sudo / root
Schaalbaarheid	Multi-user (duizenden gelijktijdige gebruikers op één systeem)	IX/UX: Oorspronkelijk single-user of beperkt multi-user (vaak per server) Windows: multi-user via AD
Audit & logging	Standaard, zeer gedetailleerd	Verschillende typen logs + SIEM
Privilege escalation	Alleen via goedgekeurde paden (APF)	Via sudo / root

Security validatie op z/OS



Marktaandeel z/OS ESMs



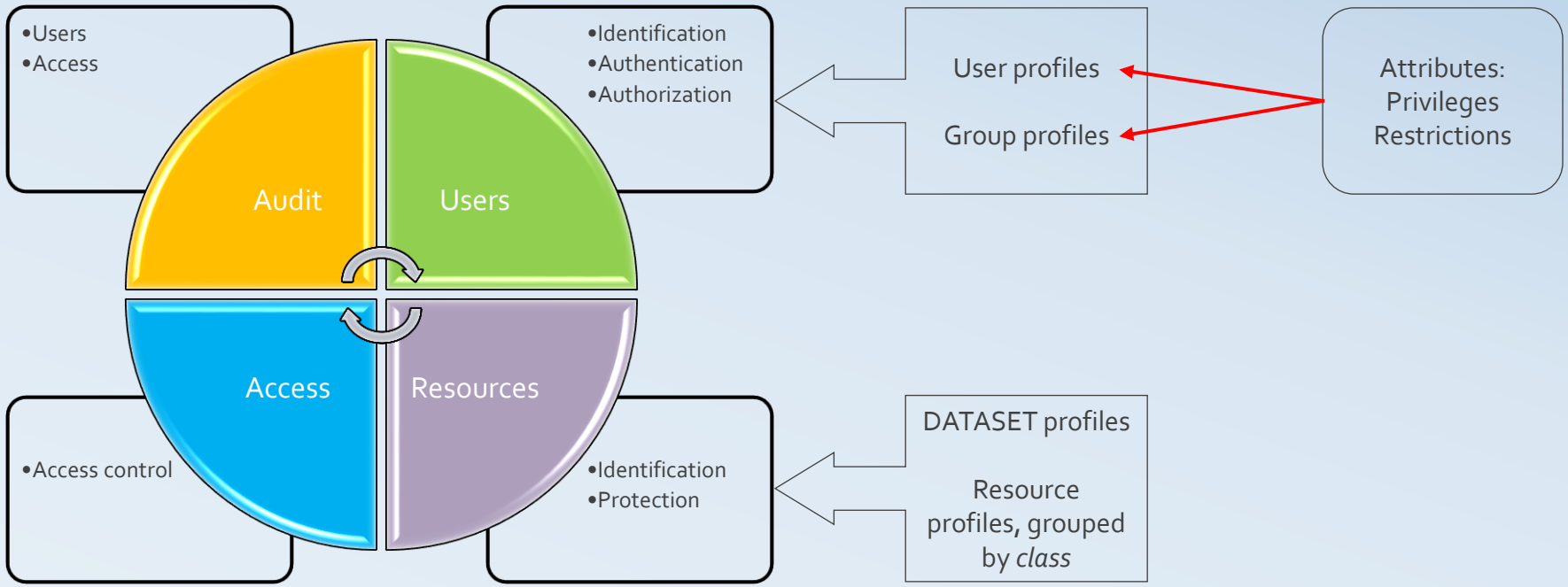
- Company size breakdown*
- > 10K medewerkers: 450+ installaties
- 5K – 10K medewerkers : ~100 installaties
- 1K – 5K medewerkers : 200+ installaties

- Sectoren*
  - Financieel + Bankwezen
  - Verzekeringen
  - Gezondheidszorg
  - Overheid
  - Overig (bijv. nutsbedrijven)

- Top 5 geïnstalleerde systemen per land *
  - USA
  - UK
  - France
  - Canada
  - Australia

* Bron: https://enlyft.com/tech/products/ibm-racf

RACF functionaliteit



Cyber attacks op z/OS

- Sterke security architectuur
- Uitgebreide logging en audit
- Weinig bekende exploits

Showing **1 - 4** of **4** results for **racf**

Show: 25 **Sort by:** CVE ID (new to old)

CVE-2016-6500 CNA: Hewlett Packard Enterprise (HPE)

Unspecified methods in the RACF Connector component before 1.1.1.0 in ForgeRock OpenIDM and OpenICF improperly call the SearchControls constructor with returnObjFlag set to true, which allows remote attackers to execute...

Show more

CVE-2011-1683 CNA: MITRE Corporation

IBM WebSphere Application Server (WAS) 6.0.x through 6.0.2.43, 6.1.x before 6.1.0.37, and 7.0.x before 7.0.0.17 on z/OS, when a Local OS user registry or Federated Repository with RACF adapter is...

Show more

CVE-2011-1321 CNA: MITRE Corporation

The AuthCache purge implementation in the Security component in IBM WebSphere Application Server (WAS) 6.1.0.x before 6.1.0.37 and 7.x before 7.0.0.15 does not purge a user from the PlatformCredential cache,...

Show more

CVE-2008-3539 CNA: MITRE Corporation

Unspecified vulnerability in HP OpenView Select Identity (HPSI) Connectors on Windows, as used in HPSI Active Directory Connector 2.30 and earlier, HPSI SunOne Connector 1.14 and earlier, HPSI eDirectory Connector...

Kwetsbaarheden uitbuiten in z/OS (ja, toch wel)

- Misconfiguraties — Foutieve RACF instellingen of access control
- Insider threats — Misbruik hoge rechten
- Indirect attacks — Via gekoppelde systemen

Maturity, governance & risks in samenhang

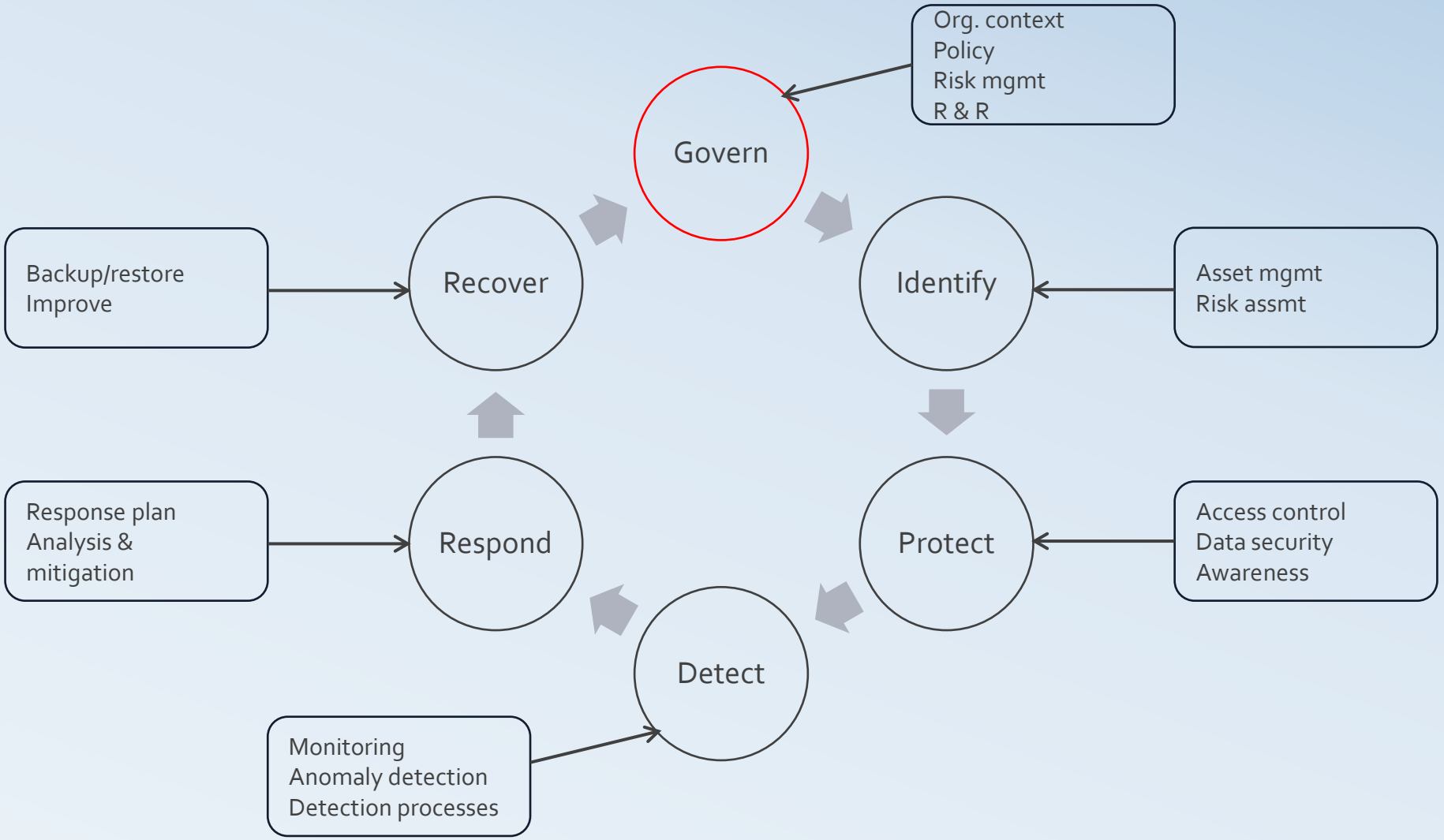
ISF Maturity Model for Information Security

Level	Capability / Activity
0 – Incomplete	Activiteit wordt niet of nauwelijks uitgevoerd; geen bewijs van uitvoering.
1 – Performed	Activiteit wordt uitgevoerd, maar zonder planning, consistentie of controle.
2 – Planned	Activiteit is gepland en gestructureerd, maar nog niet volledig beheerst.
3 – Managed	Activiteit wordt systematisch uitgevoerd, gemonitord en gecontroleerd.
4 – Measured	Activiteit wordt gemeten op effectiviteit en prestaties worden geëvalueerd.
5 – Tailored	Activiteit is geoptimaliseerd en afgestemd op specifieke risico's en context.

ISFMM: Hybrid Maturity

Level	Capability focus	Activity focus	RACF voorbeelden
0	Geen beleid, governance, ownership	Activiteit wordt niet of nauwelijks uitgevoerd	Geen RACF policy, veel SPECIAL users, geen logging
1	Security is op “best effort”, zonderstructuur	Activiteit wordt niet consistent zonder controle uitgevoerd	Er zijn basisprofielen zonder standaardisatie of review
2	Security governance is gepland	Activiteit is geland en gestructureerd, maar niet volledig beheerst	Er zijn RACF-groepen ingericht, provisioning van user accounts is beschreven
3	Security integratie met in processen met duidelijke verabntwoordelijkheid	Activiteit wordt systematisch uitgevoerd en gecontroleerd	Audit software wordt gebruikt, periodieke access reviews worden uitgevoerd
4	Security governance wordt gemeten en geëvalueerd op effectiviteit	Activiteit is gemonitord en geanalyseerd op prestaties	Full SMF logging, rapportages bv failed logins of access violations
5	Security goevernance is afgestemd op business risico’s en context	Activiteit is geoptimaliseerd en risicogestuurd	Dynamische role mapping, automatische provisioning, AI analyse van toegangspatronen

NIST CSF 2.0


Org. context
Policy
Risk mgmt
R & R
Govern
Backup/restore
Improve
Recover
Identify
Asset mgmt
Risk assmt
Response plan
Analysis &
mitigation
Respond
Protect
Access control
Data security
Awareness
Detect
Monitoring
Anomaly detection
Detection processes

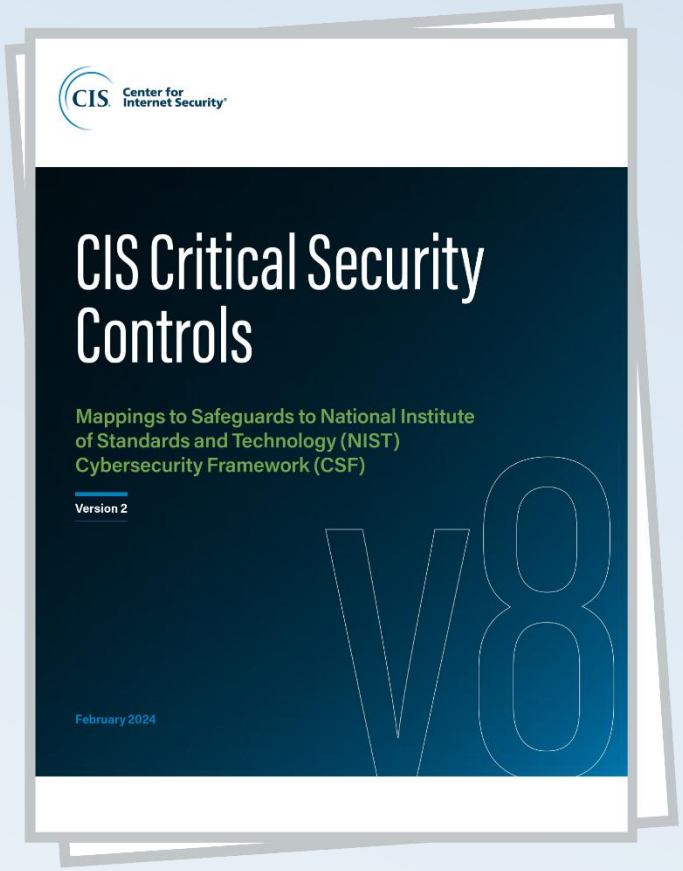
NIST CSF 2.0 Maturity Tiers - Govern

Tier	Governance-eis
1 – Partial	Governance is informeel, reactief en niet consistent toegepast. Er is weinig leiderschap, beleid of toezicht. Rollen en verantwoordelijkheden zijn onduidelijk of ontbreken
2 – Risk informed	Governance is deels gestructureerd. Er zijn beleidsregels en rollen gedefinieerd, en risicobeoordelingen worden gebruikt om beslissingen te ondersteunen. Leiderschap is betrokken, maar niet systematisch
3 – Repeatable	Governance is formeel, herhaalbaar en geïntegreerd in operationele processen. Risicobeheer is consistent en gebaseerd op beleid. Er is toezicht, documentatie en evaluatie van governanceactiviteiten
4 - Adaptive	Governance is dynamisch, risicogestuurd en continu verbeterend. Leiderschap stuurt actief op cyberrisico's, governance wordt afgestemd op strategische doelen en lessons learned worden structureel toegepast

NIST CSF – Govern + ISM MM Maturity

Level	Governance-eis	RACF voorbeelden
0	Er is geen formeel security governance proces; geen verantwoordelijkheden gedefinieerd	Geen RACF-beleid, geen eigenaarschap over profielen, privileged-rechten (special, UID=0, trusted) ongecontroleerd
1	Er is enige uitvoering van security governance, maar zonder formele structuur of consistentie	RACF-wijzigingen gebeuren ad hoc, zonder goedkeuring of logging; geen formele rollen
2	Governance is gepland met gedefinieerde rollen, verantwoordelijkheden en beleidsdocumenten	RACF-policy is opgesteld, rollen zijn toegewezen, provisioningproces is beschreven
3	Governance is geïntegreerd in operationele processen en wordt actief beheerd en gecontroleerd	RACF-wijzigingen via change management, access reviews met zSecure, logging geactiveerd
4	Governance wordt gemeten op effectiviteit en afgestemd op risicobeoordeling en prestatie-indicatoren	KPI's op policy compliance, auditrapportages over privilegegebruik en logging-analyse
5	Governance is geoptimaliseerd en afgestemd op specifieke risico's, context en strategische doelen	Dynamische role mapping, automatische provisioning, RACF governance afgestemd op business impact

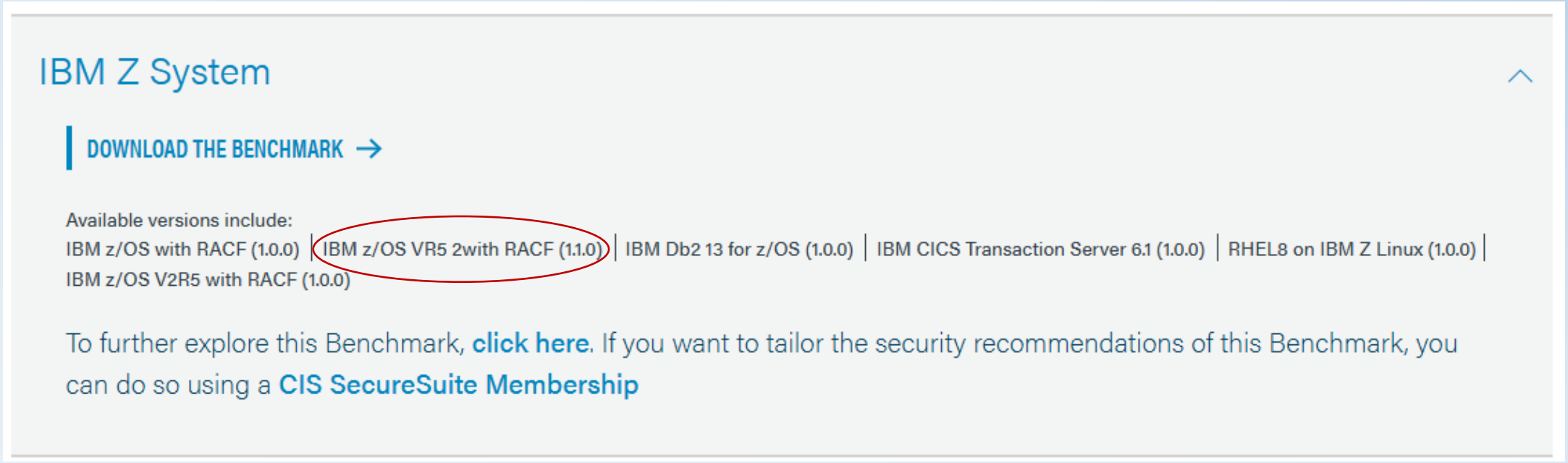
NIST ⟷ CSF controls mapping

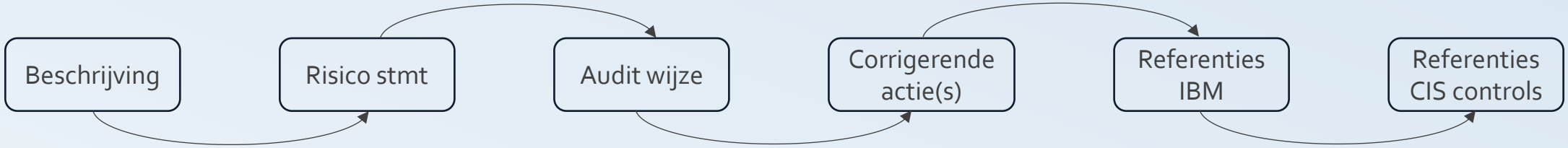


- 57 controls wederzijds mapped
- 108 CIS subcategorieën niet mapped naar NIST CSF 2.0
- 55 NIST CSF 2.0 subcategorieën niet mapped naar CIS v8

Bron: https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-nist-csf-2-0

CIS Benchmarks for z/OS





Bron: https://www.cisecurity.org/cis-benchmarks

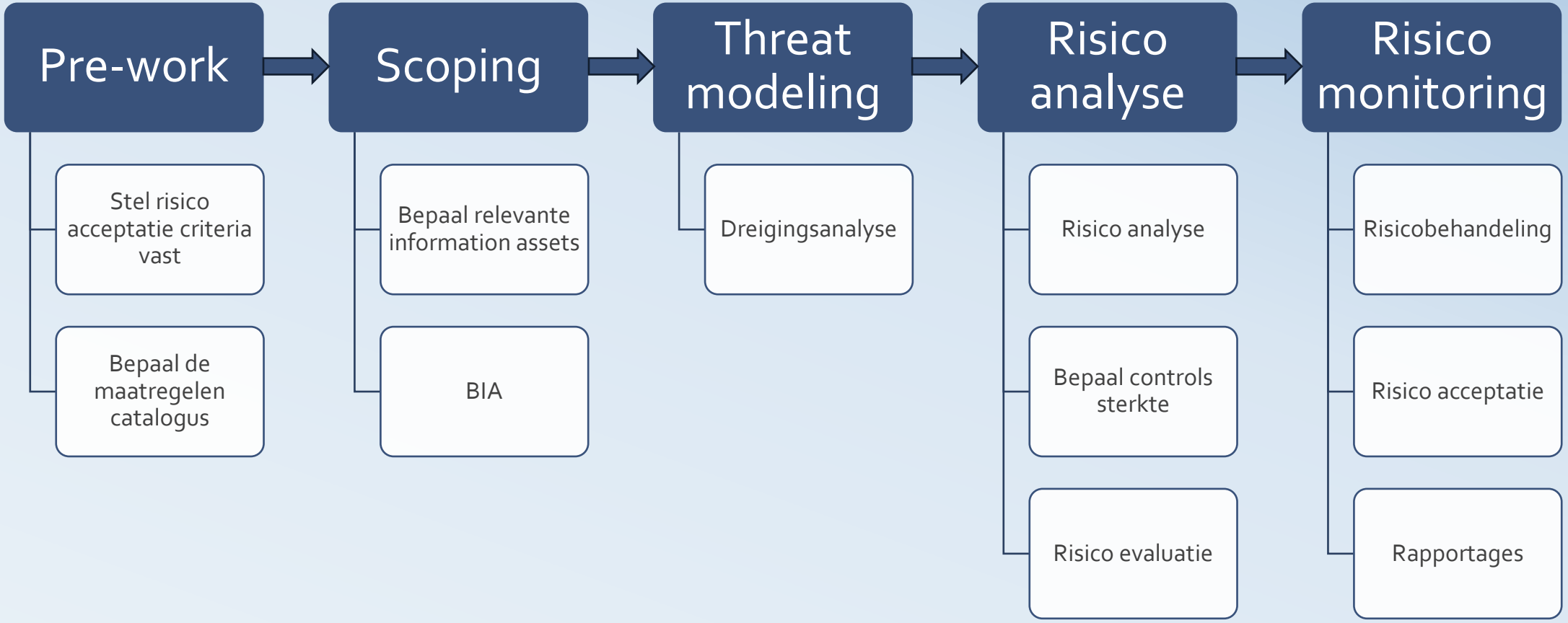
CIS Benchmark for z/OS

1: Identity & auth	2: Access control	3: Log & audit	4: Resilience	5: Storage mgmt
• 7 gebieden • 24 settings	• 4 gebieden • 48 settings	• 14 settings	• 3 settings	• 4 settings

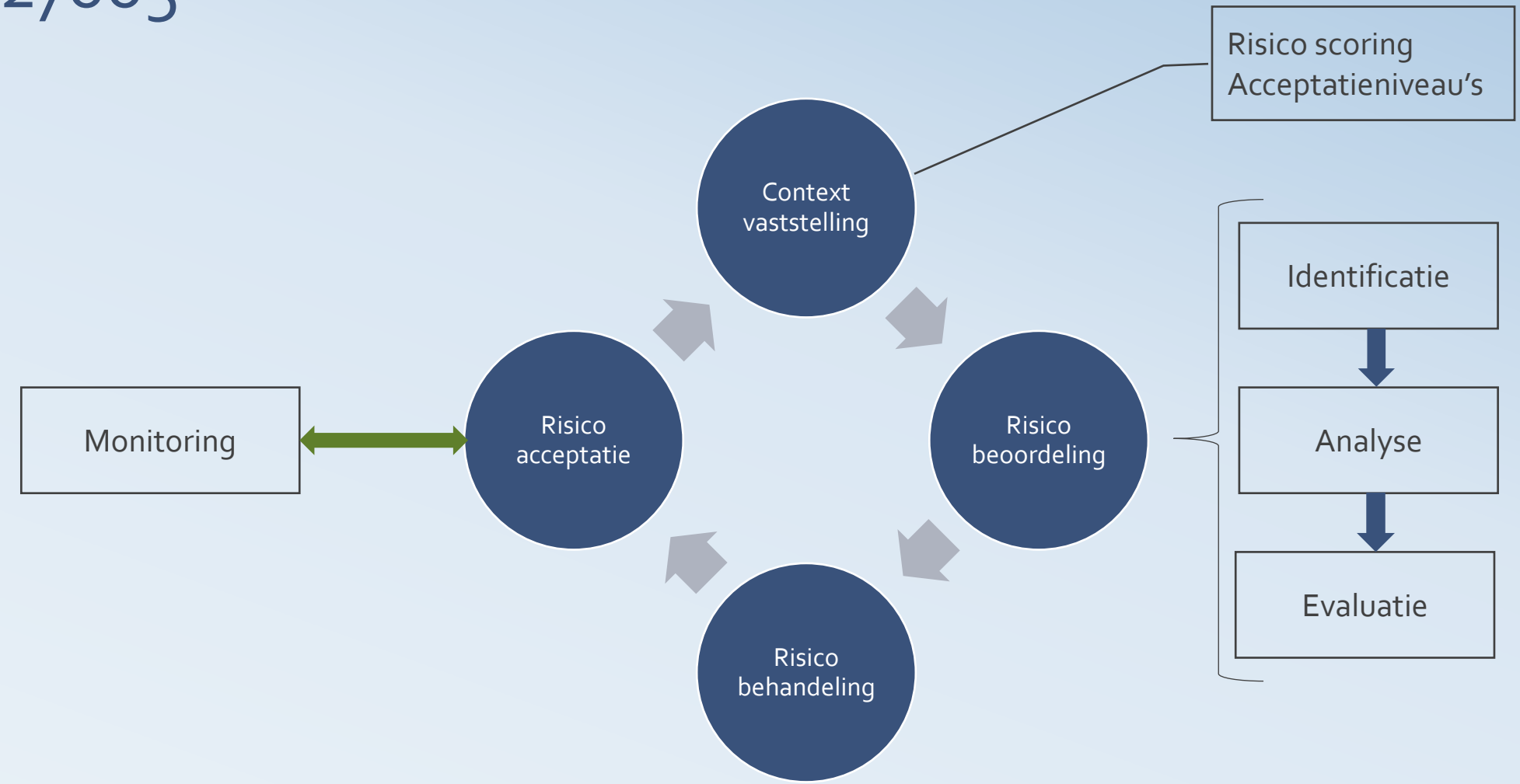
6: Network	7: Crypto	8: JES2 job mgmt	9: UNIX syst. services
• 7 gebieden • 40 settings	• 3 gebieden • 21 settings	• 8 gebieden • 32 settings	• 33 settings

In totaal 219 security settings

IRAM2


Pre-work
Stel risico acceptatie criteria vast
Bepaal de maatregelen catalogus
Scoping
Bepaal relevante information assets
BIA
Threat modeling
Dreigingsanalyse
Risico analyse
Risico analyse
Bepaal controls sterkte
Risico evaluatie
Risico monitoring
Risicobehandeling
Risico acceptatie
Rapportages

ISO 27005


Risico scoring
Acceptatieniveau's
Context vaststelling
Identificatie
Analyse
Evaluatie
Risico beoordeling
Risico behandeling
Risico acceptatie
Monitoring

Stof tot nadenken…

- Welke risico's hebben de grootste impact?

- Welke governance-gap is het meest kritisch?

Q & A

Dank!

20-11-2025

John Rudolph CIS.A/M/SP | CRISC | ISO 27001 SLI
Rudolph Infosec Consultancy
john@r-isc.nl