

Évaluez votre maturité *en cyber* *resilience des* *données.*

Rita Dib – *Security Consultant, Bechtle Suisse*

Christian Bocquet – *Senior System Engineer, Veeam*

Bechtle IT Forum, Lausanne.

24.06.2025

BITF

#BITF25





The best time to plant
a tree was 20 years ago.
The second-best time is now.

Old Proverb



veeam

Increased Risk



Gathering Cyber Storm

5 Cs of Concern

Not if, but when



World Economic Forum: Global Risks Report 2024

Global risks ranked by severity over the short term (two years)



Risk categories



Economic



Environmental



Geopolitical



Societal



Technological

1 Misinformation and disinformation

2 Extreme weather events

3 Societal polarization

4 Cyber insecurity

5 Interstate armed conflict

6 Lack of economic opportunity

7 Inflation

8 Involuntary migration

9 Economic downturn

10 Pollution



World Economic Forum: Global Risks Report 2025

Global risks ranked by severity over the short term (two years)



Risk categories



Economic



Environmental



Geopolitical



Societal



Technological

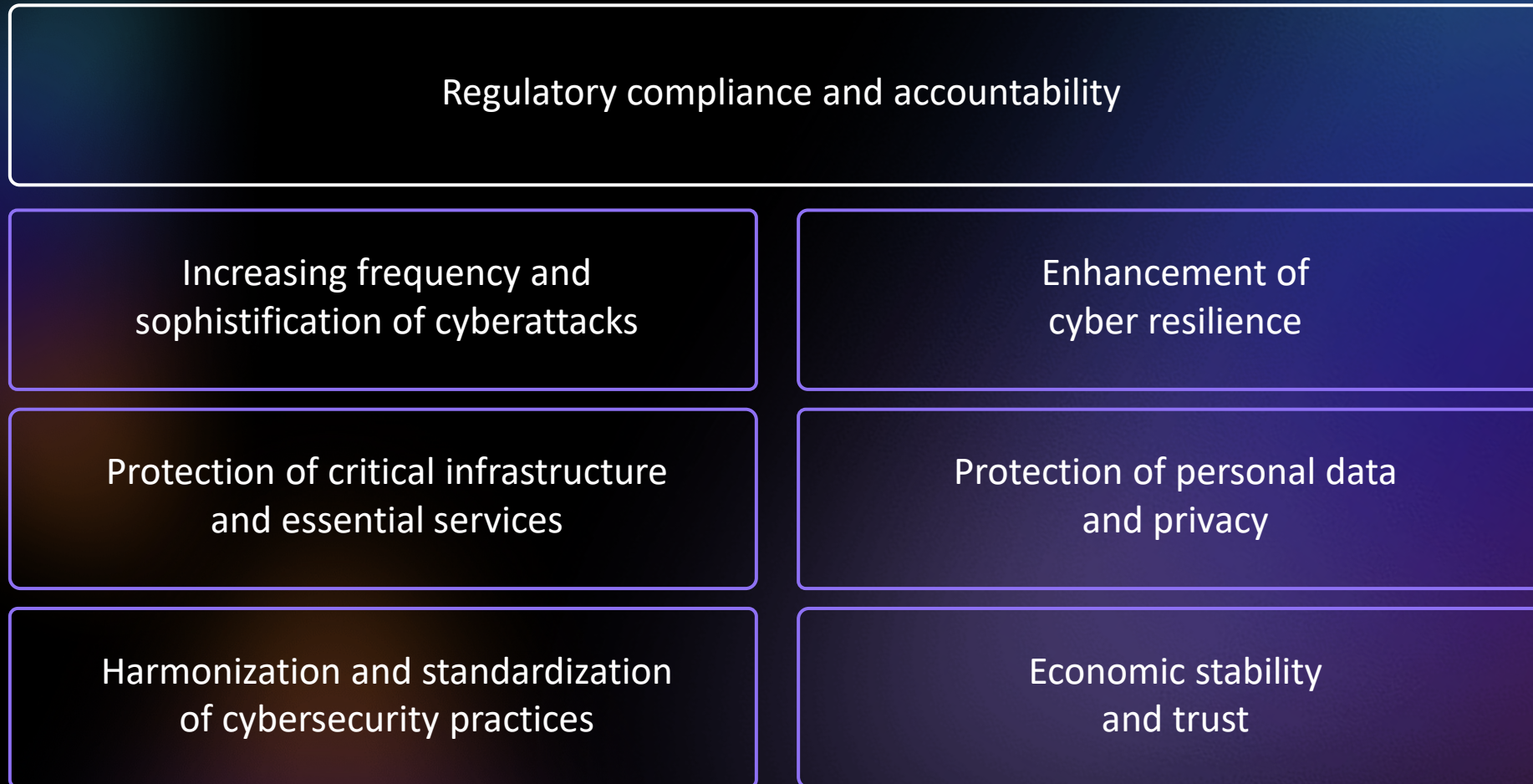
- 1 Misinformation and disinformation
- 2 Extreme weather events
- 3 State-based armed conflict
- 4 Societal polarization
- 5 Cyber espionage and warfare
- 6 Pollution
- 7 Inequality
- 8 Involuntary migration or displacement
- 9 Geoeconomic confrontation
- 10 Erosion of human rights and/or civic freedoms

Increased Expectations



What's With All These New Regulations?

Why now?



It's Not Just the EU

Cyber legislation by the numbers

167

Countries with some form of cybersecurity legislation

133

Countries with data protection regulations

97

Countries with critical infrastructure regulation



DORA

Digital Operational Resilience Act (DORA)

Key elements:



ICT risk management: Financial entities must establish frameworks to identify, protect, detect, respond to, and recover from ICT risks, including third-party dependencies.



Incident reporting: Report within strict timelines (initial notification within 24 hours).



Resilience testing: Mandates annual threat-led penetration testing and backup testing for critical systems.



Third-party oversight: Critical ICT providers (CTPPs) face direct ESA supervision with contractual and audit requirement.



Enforcement: Fines up to 2% of annual global turnover or €10 million, effective Jan. 17, 2025.



Scope: Targets EU financial sector (banks, insurers, payment providers, etc.).



NIS2 Directive

Network Information Systems Directive 2

Key elements:



Risk management: Implement technical, operational, and organizational measures to manage cybersecurity risks.



Incident reporting: Requires notification of significant incidents to national authorities, with timelines varying by impact.



Supervision: National authorities conduct audits and enforce compliance.



Enforcement: Fines up to €10 million or 2% of annual turnover, with personal liability for management.



Scope: Covers medium/large entities in 18 critical sectors (e.g., energy, health, transport).



LSI

Information Security Law (Loi sur la sécurité de l'information)

Key elements:



Risk-based approach: Obligates institutions to assess and manage information security risks proportionally to the sensitivity of data and criticality of systems.



Incident reporting: Requires federal entities to report serious security incidents to the National Cyber Security Centre (NCSC).



Third-party risk management: Mandates security requirements and monitoring for external service providers handling federal information or systems.



Enforcement: Non-compliance may lead to sanctions or operational restrictions.



Scope: Applies to Switzerland's federal administration, federal enterprises, and potentially critical private-sector organizations handling sensitive national data or infrastructure.

Key Common Principles

Principles	CERCIA	SEC	DORA	NIS2	LSI
Risk management and governance	✓	✓	✓	✓	✓
Incident response and reporting	✓	✓	✓	✓	✓
Third party risk management	✓	✓	✓	✓	✓
Resilience and business continuity	✓	✓	✓	✓	✓
Security controls and cyber hygiene	✓	✓	✓	✓	✓
Continuous monitoring and reporting	✓	✓	✓	✓	✓
Board/senior management responsibility for cyber	✓	✓	✓	✓	✓
Training and awareness	✓	✓	✓	✓	✓
Enforcement	17.01.25	18.12.23	17.01.25	17.10.24	01.01.24

What must we do ?



CONTROL

/kən'trəʊl

the power to influence or direct people's behaviour or the course of events

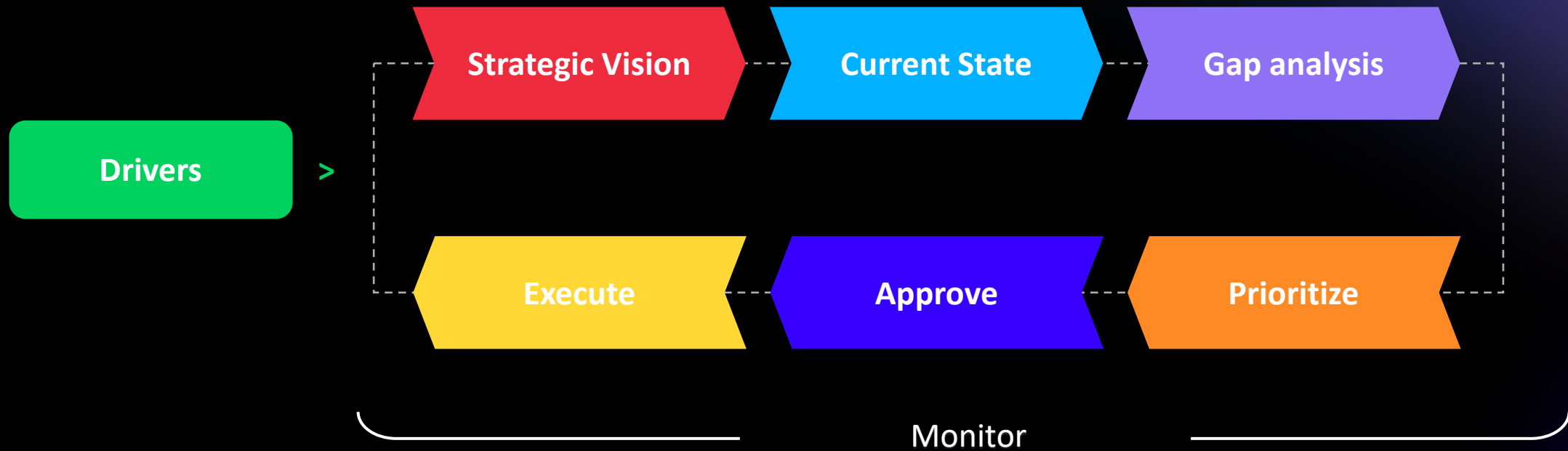


It is the responsibility of management to establish and maintain an effective system of internal control.

COSO Control Framework

Internal controls, risk management, and governance

How to Define a Security Control Approach?



What Drives a System of Internal Control?

Controls are informed by various sources (and are continuously evolving)

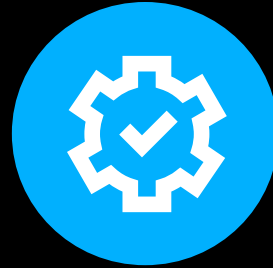
Control Environment



Business growth
enablement



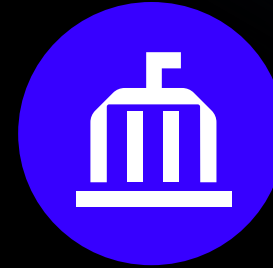
Risks and emerging
threats



Technological
advances



Laws and
regulations



Standards and
Frameworks



Policies and
Procedures

What Are Security Standards and Frameworks

Standard

Perspective rules

- Define security controls
- Compliance (certifications, laws...)
- Examples
 - ISO/IEC 27001
 - PCI-DSS
 - NIST SP 800-53

Framework

Guiding structure

- Design a cyber security program
- High flexibility (size, industry, risk...)
- Examples
 - NIST Cybersecurity Framework (CSF)
 - Secure Controls Framework (SCF)
 - COBIT

Organizations use a framework to shape their overall security program and standards to meet specific compliance or technical requirements.

What Drives a System of Internal Control?

Controls are informed by various sources (and are continuously evolving)

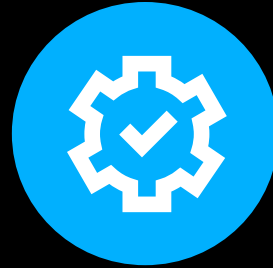
Control Environment



Business growth
enablement



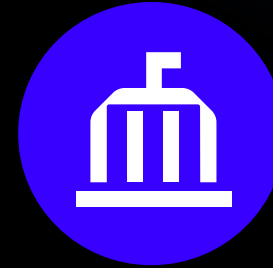
Risks and emerging
threats



Technological
advances



Laws and
regulations

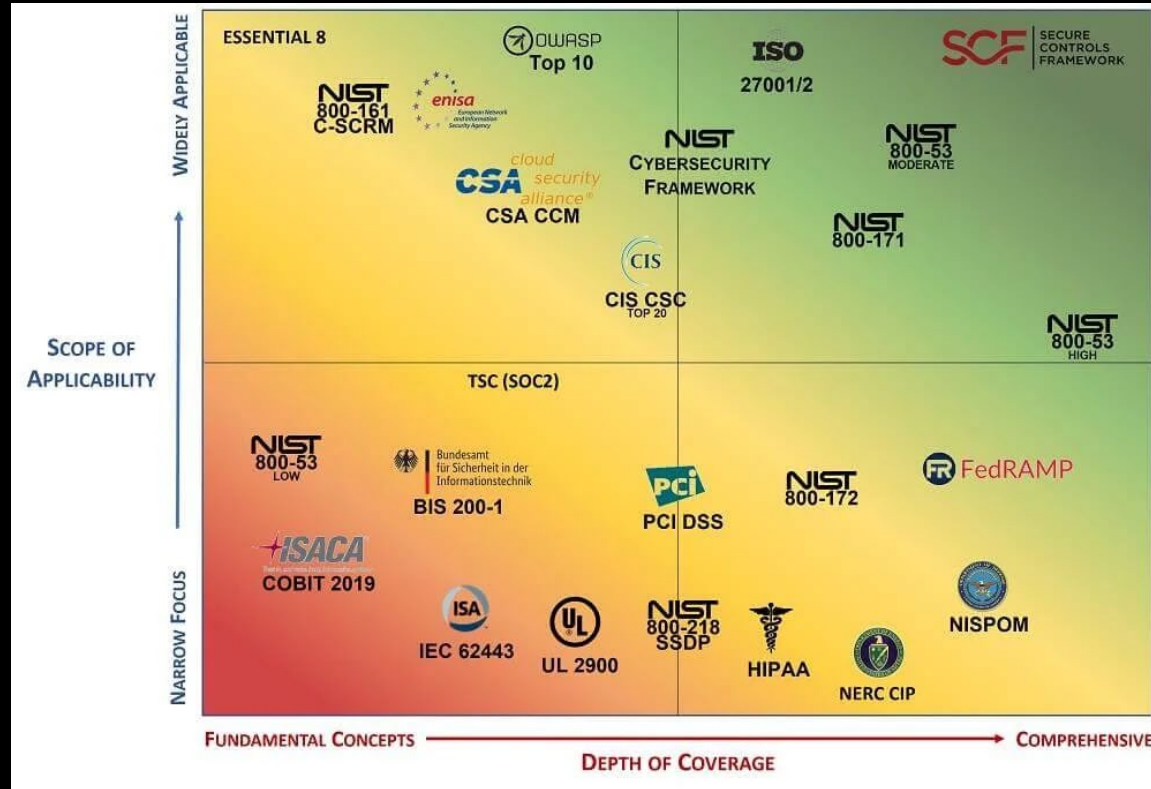


Standards and
Frameworks



Policies and
Procedures

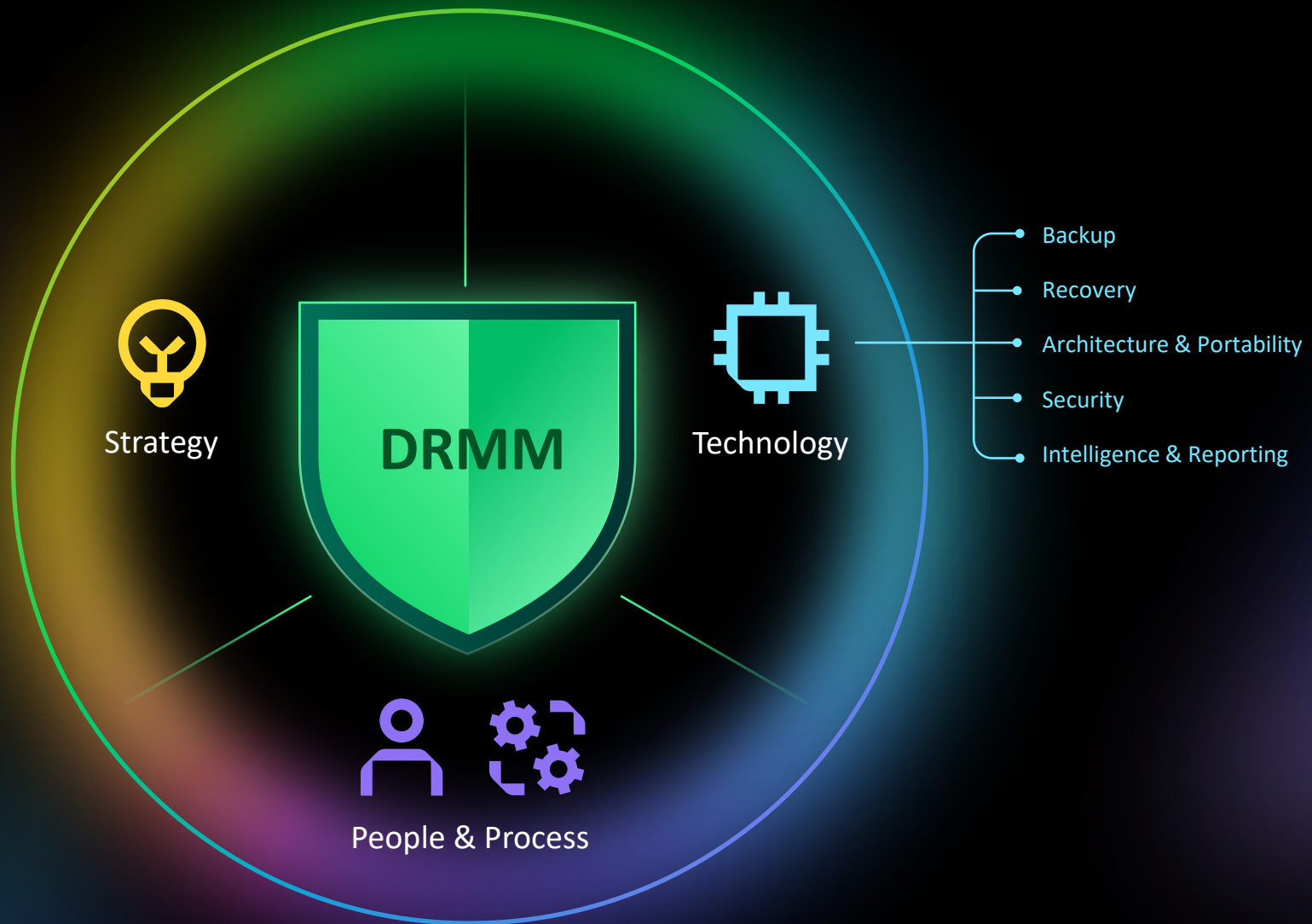
How Do You Pick A Cybersecurity Framework ?



There is no perfect framework

What work for one organization might not work well for another

Most organizations use a mix to define what right looks like



How Do We Measure the Maturity of Controls ?

Define what right looks like



Reactive
and Manual



Reliable But
Limited



Mature & Adaptive



Self Optimizing



Maturity (People, Process, Technology)

44%

Reactive & Manual

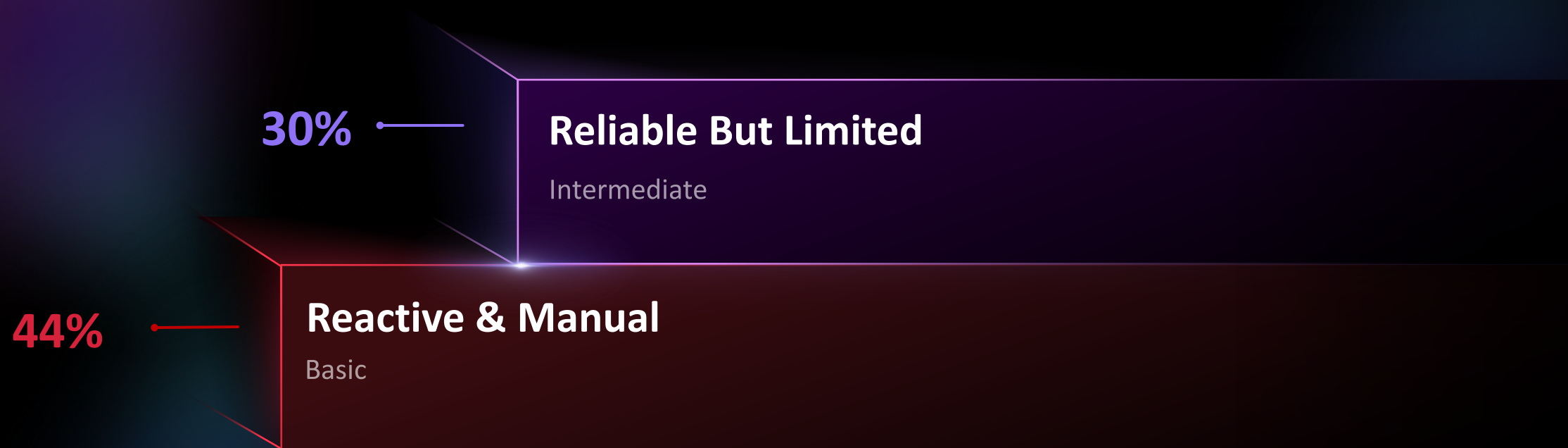
Basic

44%

- Manual backups of limited workloads
- Unclear resilience strategy
- Recovery plans = theory
- Reactive security
- Unclear accountability

Reactive & Manual

Basic



30%

RTO / RPO targets

Immutability

Retention policies

Security monitoring capabilities

Broader, but incomplete data coverage

Ransomware simulations

Reliable But Limited

Intermediate

74%

of organizations fall
into Basic and
Intermediate,
highlighting major
improvement
opportunities

30%

Reliable But Limited

Intermediate

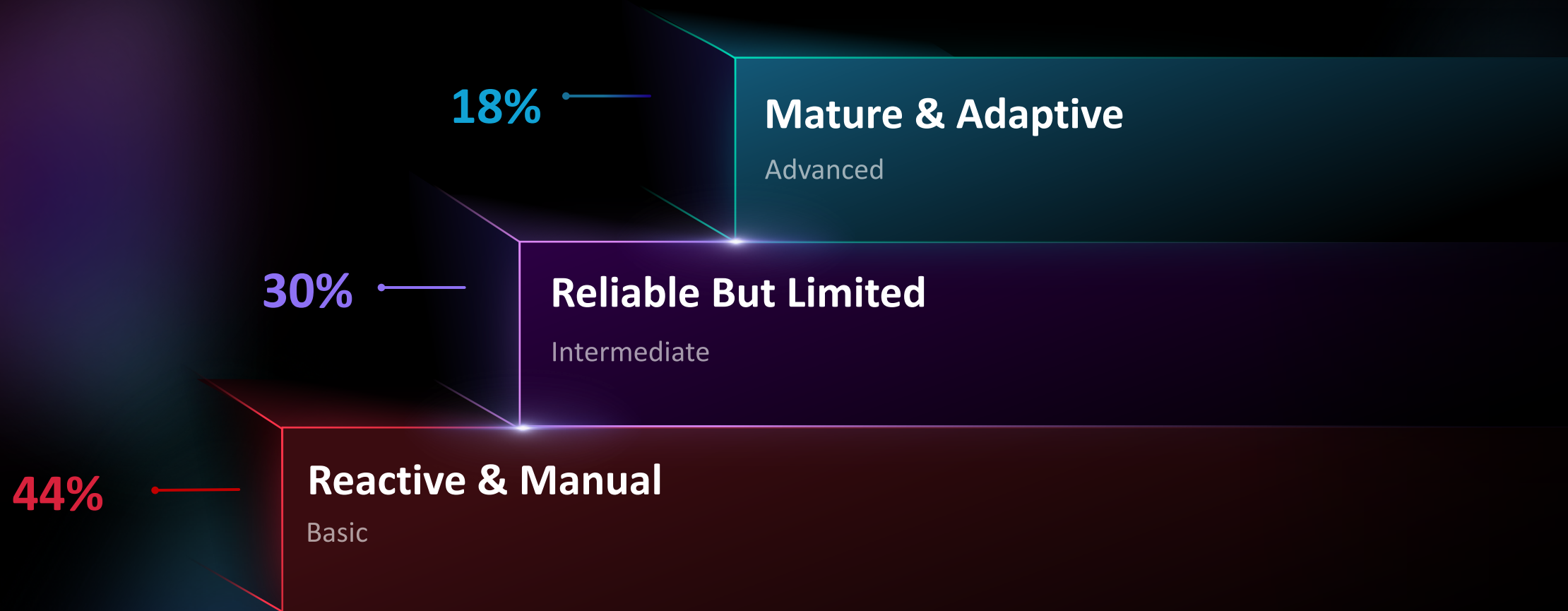
44%

Reactive & Manual

Basic



veeam



18%

- Organization-wide resilience strategy
- Complete unified workload coverage
- 3-2-1-1-0
- Advanced orchestration & automated recovery
- Cross-system, cross-environment data portability
- Integrated Security, IT, Ops
- Real-time detection
- Tested incident response playbooks

Mature & Adaptive

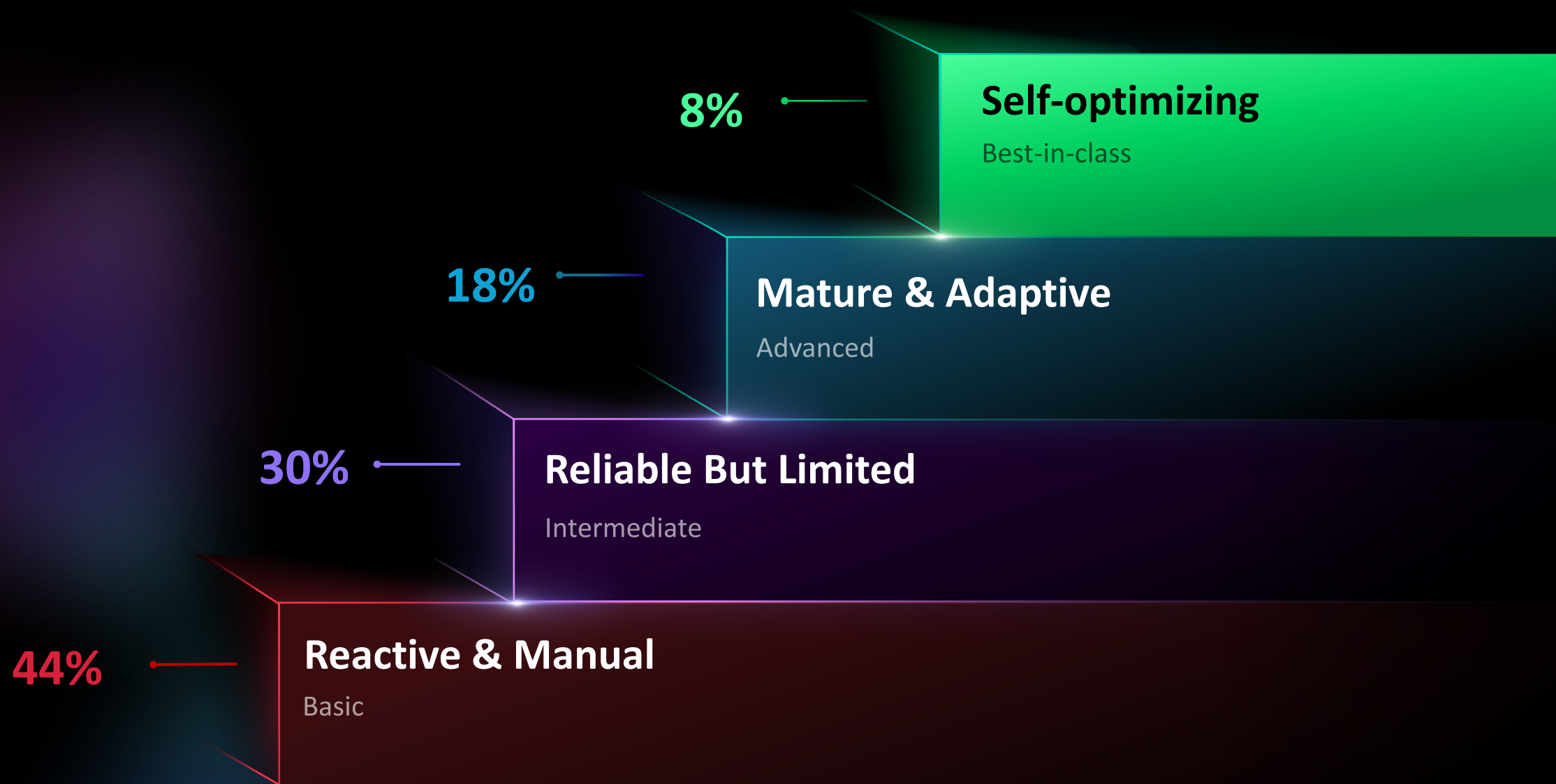
Advanced

18%

- Organization-wide resilience strategy
- Complete unified workload coverage
- 3-2-1-1-0
- Advanced orchestration & automated recovery
- Cross-system, cross-environment data portability
- Integrated Security, IT, Ops
- Real-time detection
- Tested incident response playbooks

Mature & Adaptive

Advanced

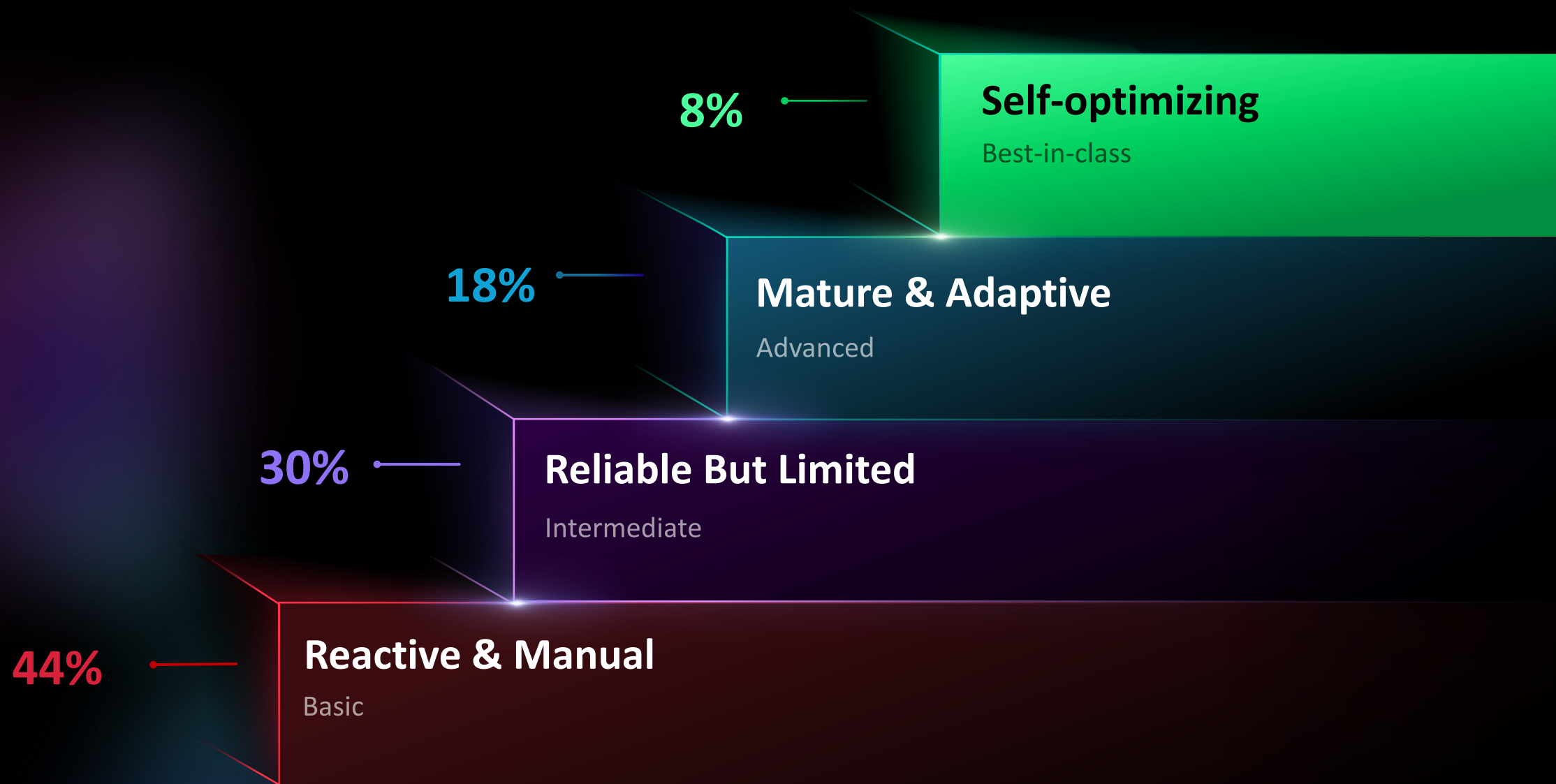


8%

Self-optimizing

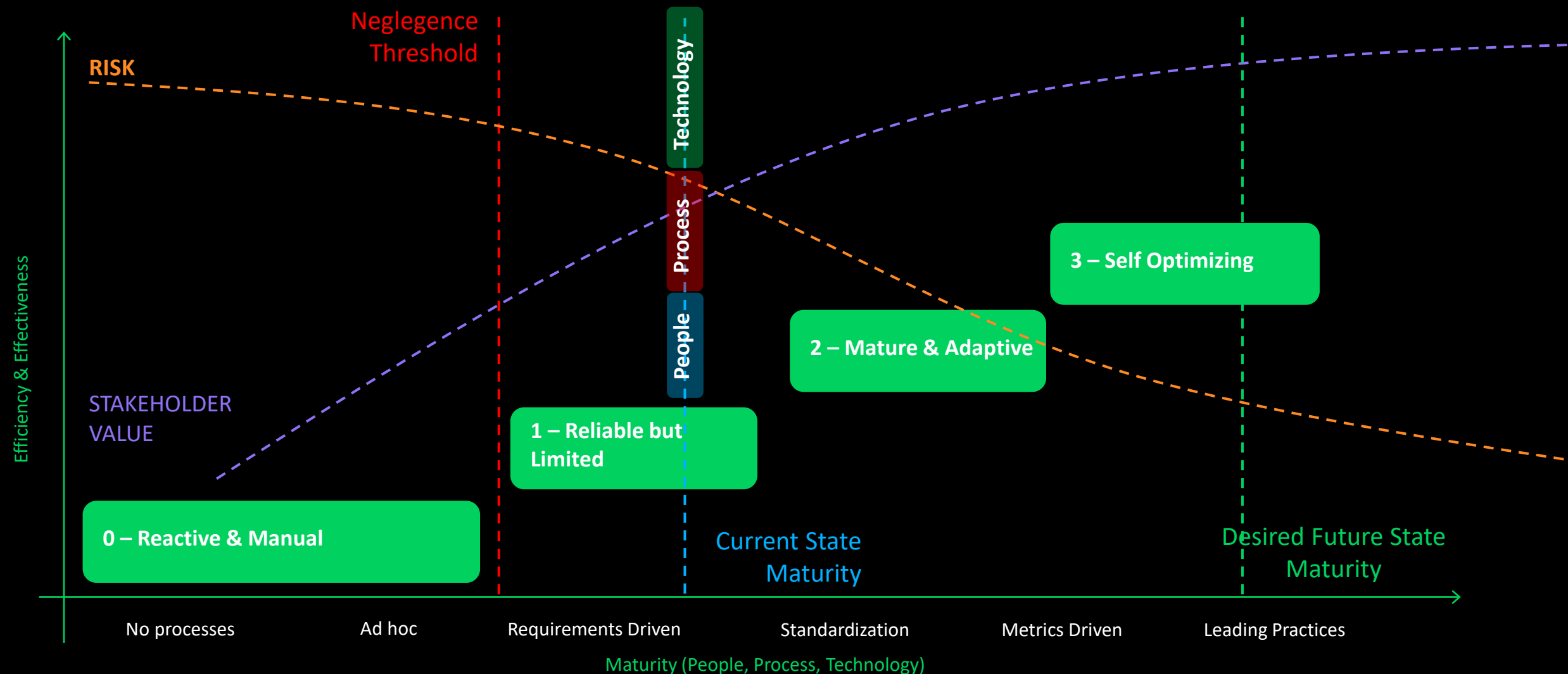
Best-in-class

- Fully automated, continuously tested Backup & Recovery
- Advanced backup techniques
- Instant cross-cloud, cross-environment, cross-region recovery
- Near-zero RTO and RPO
- Zero-trust security by default
- Advanced authentication, access control, threat intelligence
- Real-time ransomware detection and incident response
- Portable, scalable, monitored infrastructure
- AI-driven predictions and automation
- Real-time reporting and insights to action
- X-functional crisis management and readiness



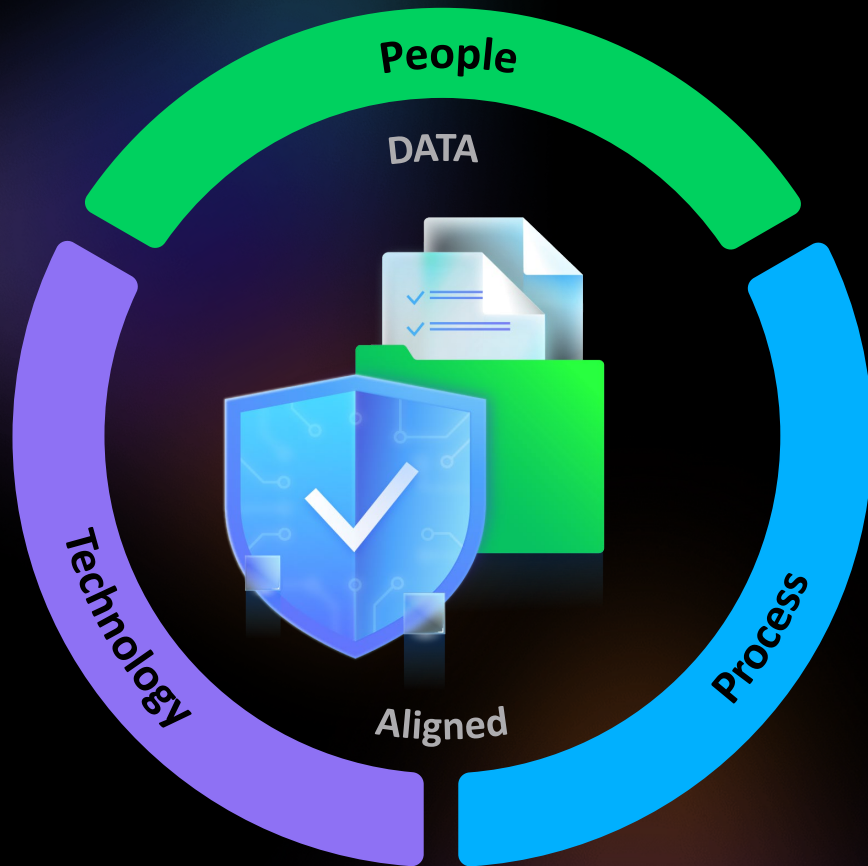
Data Resiliency Maturity Model

Define what right looks like



Transforming Compliance into Opportunity

Resiliency laws to address cybersecurity challenges



RISK

Act now or
leave to fate

RELEVANCE

Judge now or
risk the fall

REWARD

Pursue now or
miss the gain

How Does Veeam Help Out?



ICT Risk
Management



ICT Incident
Reporting



Digital Operational
Resilience Testing



ICT Third-Party
Risk Management



Information and
Intelligence Sharing



Resilience
by design



Threat intelligence and
minimize downtime
(VCS)



Proactively identify weaknesses
(technical support, PS, SA, VCS)




Organizational and
product safety



Security best practices
and VCS with TTPs
VCS quarterly

We power
data resilience,
to keep every
business running.





The best time to plant
a tree was 20 years ago.
The second-best time is now.

Old Proverb

Govern



Identify



Protect



Detect



Respond


























































Recover

Veeam Backup & Replication

Veeam ONE Monitoring & Analytics

Veeam Recovery Orchestrator

Veeam Cyber Secure

	Backup Policy		Infrastructure Inventory		Immutability		Inline Malware Detection		Discards compromised recovery point; quick restore		Instant Recovery
	Security & Compliance Analyzer		Infrastructure Assessment Report		SureBackup		Scan Backup				Secure Restore
	DR Planning / Documentation		Audit Report		Kerberos		SIEM Integration		Automatic Alarm Remediation		Staged Restore
	DR Testing		Optimizations Reports		Off-site Backups		Off-site Replicas				Granular Application Recovery
	Advanced Monitoring & Reporting		Intelligent Diagnostics		Continuous Data Protection		Possible Ransomware Activity		Ransomware Incident Response		Database and NAS Recovery
			Business View		Scale Out Backup Repository		Abnormal decrease in VM volume				Recovery to Public Cloud
			SLA Reports		MFA		Creation of new services and processes in the VM				BaaS (VCSP)
	Ongoing health assessments		Failure Modelling		Backup Copy		Suspicious incremental backup size				DRaaS (VCSP)
			Capacity Planning		BaaS / DRaaS (VCSP)						Recovery Orchestration
			Secure Design Review		Cloud Vault v2						A Ransomware Recovery Warranty covering up to \$5M USD
			Recon Scanner		Four Eyes Authorization						Support for recovery process

Cybersecurity Assessment.

Lors de cet Assessment, nous vous accompagnons dans l'analyse de votre niveau de cybersécurité et dans la définition d'une feuille de route adaptée à vos besoins.

- Questionnaire de sécurité :
 - Dérouler un questionnaire avec votre responsable de sécurité
 - Identifier les mesures en place et les lacunes de sécurité par rapport aux normes et standards de sécurité
- Audit technique :
 - Installer et configurer des outils de détection des vulnérabilités
 - Analyser les résultats
- Feuille de route :
 - Dresser une feuille de route afin d'augmenter votre niveau de protection
 - Adapter les recommandations à vos enjeux et vos besoins de sécurité
 - Estimer les budgets et ressources nécessaires pour sa mise en œuvre
- Restitution :
 - Présenter les résultats et la feuille de route aux responsables de sécurité et à la Direction

Cybersecurity Assessment.

Notre démarche combine l'évaluation de vos pratiques par notre Expert et la vérification technique des configurations pour détecter les vulnérabilités et améliorer vos défenses.



Activités et enjeux métier
Besoins de sécurité

Questionnaire de sécurité :	Audit technique :
Evaluation des pratiques de sécurité selon les standards (ISO27001)	Installation et configuration d'outils et des scripts d'audit
Questions / Réponses	Analyse des vulnérabilités remontées
Déclaratif	Périmètre : Endpoint, Active Directory, Entra ID, Network, M365, Azure

Attribution d'une note du niveau de protection actuel
Identification du niveau cible

Feuille de route ambitieuse, mais atteignable
Priorisation des actions en fonction de la criticité et la complexité
Estimation du budget et des ressources nécessaires
Validation avec l'équipe IT et sécurité

Restitution à la Direction pour obtenir leur validation et leur appui de la démarche de sécurité

Merci!

Des questions ? Contactez-nous :
it-forum.ch@bechtle.com

