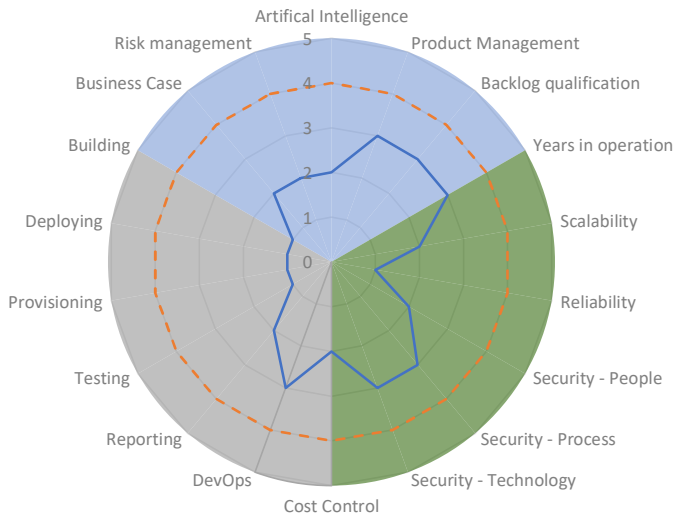
IT VALUE SCAN

Angle	Category	score	Goal	Max
Doing Right Things	Business Case	2	4	5
	Risk management	2	4	5
	Artifical Intelligence	2	4	5
	Product Management	3	4	5
	Backlog qualification	3	4	5
	Years in operation	3	4	5
Doing Things Right	Scalability	2	4	5
	Reliability	1	4	5
	Security - People	2	4	5
	Security - Process	3	4	5
	Security - Technology	3	4	5
	Cost Control	2	4	5
Doing Things Fast	DevOps	3	4	5
	Reporting	2	4	5
	Testing	1	4	5
	Provisioning	1	4	5
	Deploying	1	4	5
	Building	1	4	5



DOING RIGHT THINGS

	Business Case	Risk Mngt	AI	ProductMngt	Backlog	Years in operation
LEVEL 5	Prediction: System suggests measurements based on actuals and forecast	Optimized: Integrated risk management incl. Risk appetite, tolerances, KRIs and predictive analytics	Transformational: AI is part of business DNA	Mature Suite: Product management only based on quantitative analysis. R&D through acquisitions	User Voice	End of Live / Phase-out
LEVEL 4	Forecast: The business case reports are generated automatically and include a forecast based on actuals.	Managed Systematic: Integrated Risk Management including Qualitative and Quantitative analysis	Systemic: AI is pervasively used for digital process and chain transformation, and disruptive new digital business models	Scaled Product: Product management only based on quantitative analysis only	More business (new service)	> 2 years
LEVEL 3	Automated: The business case reports are generated automatically and can be reviewed anytime.	Top Down Repeatable: Systems in place to monitor critical risks	Operational: AI in production, creating value by process optimization or product / service innovations	Business Case Validated: Design and product management, add customer types and functionality	Improve business case	2 years
LEVEL 2	Periodically: There is a business case which is being evaluated at least every year. Overview is created manually.	Initial Siloed: Repetitive qualitative risk analysis on every business case	Active: AI experimentation, mostly in a data science context	Product / Market Fit: Business model, value proposition, platform, functionality	Existing contract requirements	1 year
LEVEL 1	Initial: There is no financial business case or it has been made initially but not updated over time	AD-HOC: Manual risk analysis, no supporting systems in place	Awareness: Early AI interest with risk of overhyping	Startup: Research, design, product mngt and possibly some engineering	Laws and regulations	< 1 year

Business Case	2
Risk management	2
Artifical Intelligence	2
Product Management	3
Backlog qualification	3
Years in operation	3

DOING THINGS RIGHT

			SECURITY			
	Scalability	Reliability	People	Process	Technology	Cost Control
LEVEL 5	Multi-tenant with loadbalancing and auto-scalability features to handle (peak) load (microservices)	0-1 prod incident / year	Culture supports continuous improvement to security skills, process, technology	Processes more comprehensively implemented, risk-based and quantitively understood	Controls more comprehensively implemented, automated and subject to continuous improvement	Pro-active automated advices to lower the costs per (micro) service
LEVEL 4	Multi-tenant with load balancing features to distribute load	2-3 prod incidents / year	Increased resources and awareness, clearly defined roles and responsibilities	Formal infosec committees, verification and measurement processes	Controls monitored, measured for compliance, but uneven levels of automation	Regular cost savings are executed. Costs per operational unit are continuously going down.
LEVEL 3	Single instance for all clients, customizing through metadata	5-8 prod incidents / year	Some roles and responsibilities established	Organization wide processes and policies in place but minimal verification	More controls documented and developed, but over-reliant on individual efforts	Cost control is embedded in DevOps process
LEVEL 2	Separate application instance for each client but customizing available by changing settings	8-12 prod incidents / year	InfoSec leadership established, informal communication	Basic governance and risk management process / policies	Some controls in development with limited documentation	Cost for Resource Group and / or (Micro) Service are known but not linked to value streams / departments
LEVEL 1	Separate application instance for each client (monoliths)	> 12 production incidents / year	Activities unstaffed or uncoordinated	No formal security program in place	Activities unstaffed or uncoordinated	Cost for Resource Group and / or (Micro) Service are unknown

Scalability	2
Reliability	1
Security - People	2
Security - Process	3
Security - Technology	3
Cost Control	2

DEVOPS MATURITY MODEL

	DevOps	Reporting	Testing	Provisioning	Deploying	Building
LEVEL 5 Complete	Operations and development are both part of the multidisciplinary delivery team and share responsibilities	Reports also provide trend analysis.	100% fully automated tests all the way to production	Self Service portal for requesting an environment.	Continuous end-to-end deployments	End-to-end automated gated builds.
LEVEL 4 Advanced	An envoy of operations works along in project, an envoy of development works along with operations.	Dashboard provides insight from different perspectives and shows history and progression through a build monitor to all	Automated dynamic quality tests like security scans, functional and performance tests guarantee quality of code.	Environment can be created and torn down by a push of the button. Operating System is virtualized.	Test-gated deployments of end-to-end applications. Deployments occur over multiple environments.	Central build environment. Teams actively reuse generic components in a secure and controlled manner.
LEVEL 3 Average	Development and operations work together when this is required	Graphical and textual reports accessible through dashboard.	Automated static code and security analysis after code check in.	Environments are identical. Several tools used to provision and configure an environment.	Environments are identical. Roll out of applications performed by a push of the button. Auto-deployment to DTAP.	Build on commit. Archived components are made available for reuse by other teams.
LEVEL 2 Beginner	Code accompanied with release notes with which operations should install and manage the application.	Reports generated on request by system administrator. Reports are graphical in nature.	Automated tests are initiated as soon as code is checked in. Tests are focused on unit/ component testing only.	Scripted installations per component for each server. Surrounding systems manually configured.	Self service deployments to development and test.	Automated builds are performed in a central area and activated manually.
LEVEL 1 Base	Operations engaged at the end of the project	Reports generated on request by system administrator. Reports are text based.	All tests require manual activity. Some tests are automated but have to be installed by hand.	Manual installation and configuration of software for middleware, databased, applications servers, etc.	Deployment through execution of separate deployment- and db scripts. Manual configurations and installs / env.	Builds are performed on local workstation by use of one or more separate build scripts.

DevOps	3
Reporting	2
Testing	1
Provisioning	1
Deploying	1
Building	1