Navigating DevOps Requirements with Risk Management

Victoria (Vicky) Hailey, CMC
VHG-The Victoria Hailey Group Corporation

vicky@vhg.com www.vhg.com https://www.linkedin.com/in/vhgcorp/ +1 416-410-3400

What DevOps Requirements?

- DevOps requirements include:

  Volume + Velocity + Variety + Veracity +

  Volatility + Visibility + Variability + Value +

  Validity + Visualization +

  + All the business requirements

That's not possible at Level 1!
DevOps, and by extension, DevSecOps, requires higher process capability than the typical IT shop

What DevSecOps Requirements?

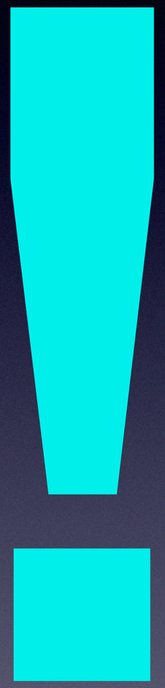
DATA / BIG DATA QUALITY NOW FACTOR INTO TRUST & DECISION-MAKING

- DevSecOps has additional fundamental infosec requirements to be concerned with:
  - Confidentiality (+ Anonymization, Encryption +++)
  - Integrity (+ Non-repudiation, Accuracy, Data Quality +++)
  - Availability (+ Accessibility, Response Time, Up-time +++)
  - Privacy (where applicable)

To manage DevSecOps, the DevOps business and stakeholder context must be known, understood, and actively managed.

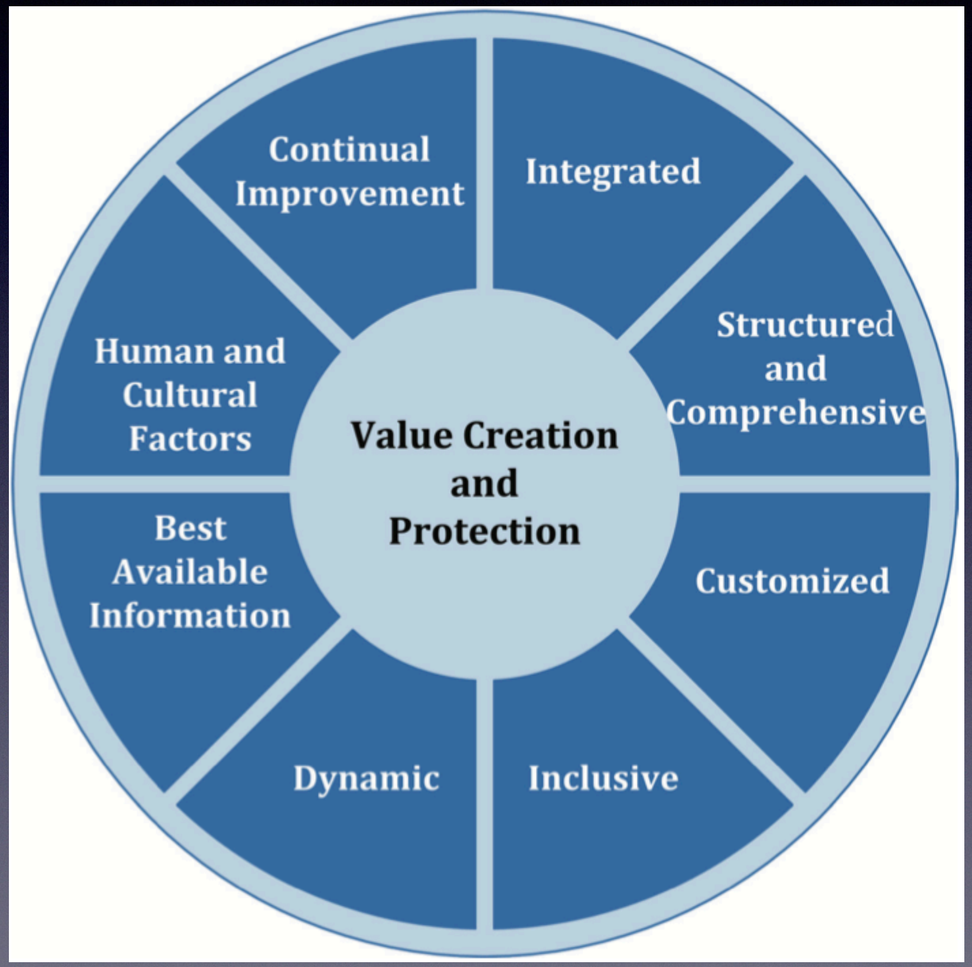
Risk Management is *Overarching*

- DevOps objectives map the V requirements to the business objectives
- Risk: ***the effect of uncertainty on objectives***
  (ISO 31000, ISO/IEC/IEEE 16085)
- Managing risk becomes the overarching process that:
  - enables integration across all stakeholder groups
  - crosses all levels of the organization
  - focuses on always knowing how close to the guardrails the targets and outcomes are
- Risk decisions can/should be automated, with direct traceability to requirements
- Risk thresholds determine when manual intervention in decisions or approvals is required



Risk Principles

- Sets the stage for the management of risk across all functions (cross-functional deployment)
- Ensures a common understanding on how to approach risk
- Establishes the approach for everyone within the organizational system, including the governing body, management, the DevOps team, stakeholders, and suppliers.



ISO 31000:2018

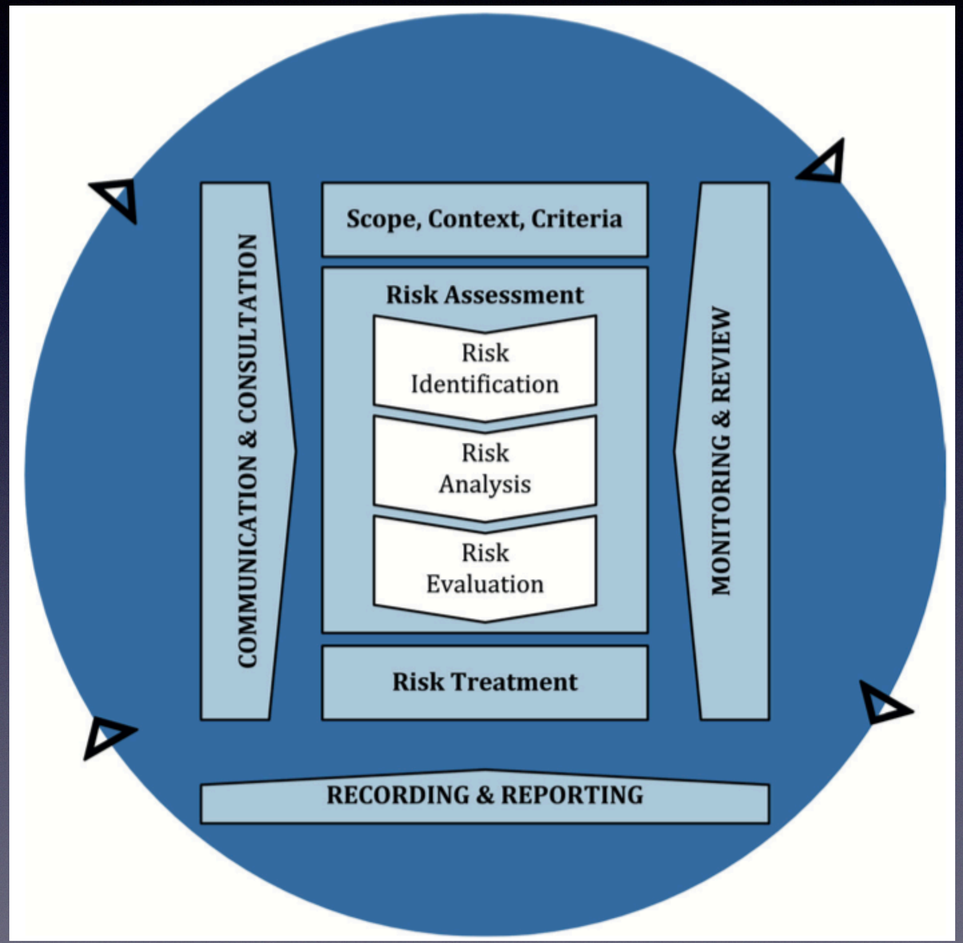
Risk Framework

- The risk framework keeps everyone on the same page
- "*The purpose of the risk management framework is to assist the organization in integrating risk management into significant activities and functions. The effectiveness of risk management will depend on its integration into the governance of the organization, including decision-making. This requires support from stakeholders, particularly top management.*" ISO 31000:2018
- The iterations enable DevSecOps to integrate seamlessly into DevOps
- Integration through to improvement keep the focus on requirements.

ISO 31000:2018

Risk Process

- Applies to all levels:
  - strategic
  - operational
  - programmes
  - projects.
- Applies to all processes, changes, suppliers
- Changes according to the specific context.
- The risk process must be iterative, repeating as often as risk tolerances demand.



ISO 31000:2018

Higher Capabilities Required

- High-capability DevOps requirements create the delta of high-capability requirements for *DevSecOps* to meet
- Meeting Volume, Velocity, Variety, Veracity, Volatility, Visibility, Variability, Value, Validity, Visualization requirements create ***Vulnerabilities against which DevSecOps must safeguard***
- Achievement of DevOps outcomes is only possible by managing the risks, including process risks, that ensure the outcomes meeting the V requirements can be met.

Thank you!

Questions?