Dear Auditor

DevOps Community
to Security with Love

IT REVOLUTION
DEVOPS ENTERPRISE FORUM
2018

IT REVOLUTION

25 NW 23rd Pl
Suite 6314
Portland, OR 97210

Dear Auditor: DevOps Community to Security with Love

Produced in the United States of America

Cover design and interior by Devon Smith

For further information about IT Revolution, these and other publications, special discounts for bulk book purchases, or for information on booking authors for an event, please visit our website at ITRevolution.com.

Preface

In March of this year, we at IT Revolution once again had the pleasure of hosting leaders and experts from across the technology community at the DevOps Enterprise Forum in Portland, Oregon. The Forum's ongoing goal is to create written guidance to overcome the top obstacles facing the DevOps enterprise community.

Over the years, there has been a broad set of topics covered at the Forum, including organizational culture and change management, architecture and technical practices, metrics, integrating and achieving information security and compliance objectives, creating business cases for automated testing, organizational design, and many more. As in years past, this year's topics are relevant to the changing business dynamics we see happening across all industries and the role technology has to play within those changes.

At the Forum, as in previous years, participants self-organized into teams, working on topics that interested them. Each team narrowed their topics so that they could have a "nearly shippable" artifact by the end of the second day. Watching these teams collaborate and create their artifacts was truly amazing, and those artifacts became the core of the Forum papers you see here.

After the Forum concluded, the groups spent the next eight weeks working together to complete and refine the work they started together. The results can be found in this year's collection of Forum papers.

A special thanks goes to Jeff Gallimore, our co-host and partner and co-founder at Excella, for helping create a structure for the two days to help everyone stay focused and productive.

IT Revolution is proud to share the outcomes of the hard work, dedication, and collaboration of the amazing group of people from the 2018 DevOps Enterprise Forum. Our hope is that through these papers you will gain valuable insight into DevOps as a practice.

—Gene Kim
June 2018
Portland, Oregon

April 14, 2018

The DevOps Community
Every DevOps IT Department
Anywhere, The World

Dear Auditor,

We realize that we have been rapidly changing our practices from Agile and DevOps to cloud and containers. Yes, we have been busy, and we are having great success delivering faster than ever with better quality and responsiveness to competitive pressures. This isn't just icing on the cake; the only sustainable advantage in our industries is the ability to meet customer demands faster and more reliably than our competitors.

But with all this growth, we made a mistake: we forgot to bring you along for the ride. That is totally our bad, but we want to make it right. We are going to make some new commitments, including the following:

- We will bring you along.
- We will be fully transparent with you about our development process.
- We realize that we own the risks of our business, and we will act accordingly.
- We will maintain an open channel of discussion to demonstrate to you how we manage risks with our modern development practices.

For example, you have told us that you are concerned about the separation of duties in Agile and DevOps practices, and we heard you! We have a better way to manage this issue now. Maintaining version control for everything we work on, enforcing peer review for all changes, releasing via a secure pipeline, restricting production access, and monitoring unauthorized changes in production systems should address your concern.

The DevOps community has been experimenting quite a bit over the last several years, and common practice now represents the collective wisdom across many companies, industries, and countries.

We have compiled a list of audit concerns and documented them in a Risk Control Matrix with lots of details about the controls, our practices, and evidences that have been collected to support each control. We hope this matrix provides a way for us to collaborate on risk mitigation practices from now on.

We are not in any way backing down from our commitment to providing value at a fast pace; rather, we are regrouping in order to improve our processes, and we are truly excited to move forward—together.

Excelsior,
The DevOps Community

Attachment:
Risk Control Matrix

Risk Controls Matrix

We Will Manage This Risk	By Performing These Activities	Which Fulfill These Controls
Unauthorized changes to production	Making sure the right people are making the changes through: • Multi-factor authentication • Role-based access control • Managing all credentials, tokens, connection strings, endpoints, and other secrets in an encrypted vault and rotating them on a period basis or upon relevant business events (such as employee separation) Assuring that changes can’t be made manually by ensuring: • No human access to production except by time-limited tokens granted under access approval rules (“just-in-time admin”) • All change events are logged and monitored • Production changes are made only via secure pipelines (inputs to the pipeline are known and reviewed, and changes to the pipeline steps are reviewed and approved)	Identity management, centralized access management, encryption, secrets management, separation of domains, secure pipelines

	Data is protected and isolated through: • Data encryption in rest and in transit • Separation of networks and domains Our development practices are representative of the responsible work of our craft; for example: • All sources (infra, app, tests, policies, and pipeline) are version-controlled under permissions • All changes to sources are peer reviewed • Critical business transactions are tested in production • Incident response processes have service-level expectations	
Production breaks due to human error or untested/ insecure code	• All sources (infra, app, tests, policies, and pipeline) are version-controlled under permissions • All changes to sources are peer reviewed • Deployment authorization • Automated software composition analysis • Automated static code analysis	Test traceability, test results (including security tests and scans)

	• Automated dynamic analysis • Automated security BDD with evil user stories • Automated “Chaos” testing (like Google’s Chaos Monkey, etc.) • Product team fully accountable for quality of service in production	
Material misstatement of financial data	• Segregate financially relevant systems and services • Authorized code review (who, what, where) • Rotation of job responsibility • Code ownership at a team level • Anomaly detection • “Just-in-time admin”	Least privilege access code review, four eyes on code and deployment
Intellectual property and licensing violation (open source/commercial)	• Software composition analysis • Approved software inventory • Bill of materials on every build	Verification of authorized software
Data breach from unauthorized access	• Full definition (PII) tokenization • Encryption at rest and in transit • Data retention policy	Compromise from insider threat

	• Ethical hacking, “red teaming” to identify vulnerabilities on a regular cadence	
Unwanted customer impact (blast radius) from changes	• Canary deployment • Exposure control through progressive blue/green deployment • Features flags for dark launches and experimentation • In absence of exposure control, automated rollback process • A/B testing	
Business continuity	• Continuous data replication off site • Secondary hot site • RTO/RPO acceptance from business • Periodic disaster recovery exercise	Timely backup and recovery
Divergence of audit evidence from developer evidence	• Automated evidence and log collection across toolchain with traceability and tagging for extraction • Reproducibility of the version of product state	Valid source documents with completeness and accuracy

Violation of GDPR (General Data Protection Regulation of the European Union) or leak/misuse/retention of PII against rules	• Hosting data in appropriate jurisdiction • Allowing EUII deletion • Plain-language terms and conditions	Data residency, right to forget, customer awareness of T&C
Hidden compromise or unknown breach of infrastructure	• Ethical hacking, “red teaming” to identify vulnerabilities on a regular cadence • Monitoring data egress • Attack detection • Instrumentation to capture unusual activities	Appropriate management of cyber-risk

CONTRIBUTORS

- Ben Grinnell, Managing Director and Global Head of Technology & Digital, North Highland
- James Wickett, Head of Research, Signal Sciences
- Jennifer Brady, Technology Governance Director, Capital One
- Robert Stroud, Chief Product Officer, XebiaLabs
- Sam Guckenheimer, Product Owner of Microsoft Visual Studio
- Scott Nasello, Director, Delivery Engineering, Columbia Sportswear
- Tapabrata Pal, Senior Director & Senior Engineering Fellow, Capital One