QR SOLVE

DevOps automation

DevOps activities

01 CI/CD Pipelines

Identify, design and implement integration flow for microservice or microfrontend component

02 Infrastructure as Code

Reflect and implement system architecture as source code definition using programming language

03 Software adaptation

Check and optionally adapt software platform to be ready for automation and cloud deployment

04 Tests & monitoring

Automate existing test cases or create new automation tests compliance with test pyramid and modern frameworks

CI/CD Pipelines

A NoOps environment means no operations. NoOps is when an IT environment becomes so automated from the underlying infrastructure through technologies.

01 CI/CD process designing

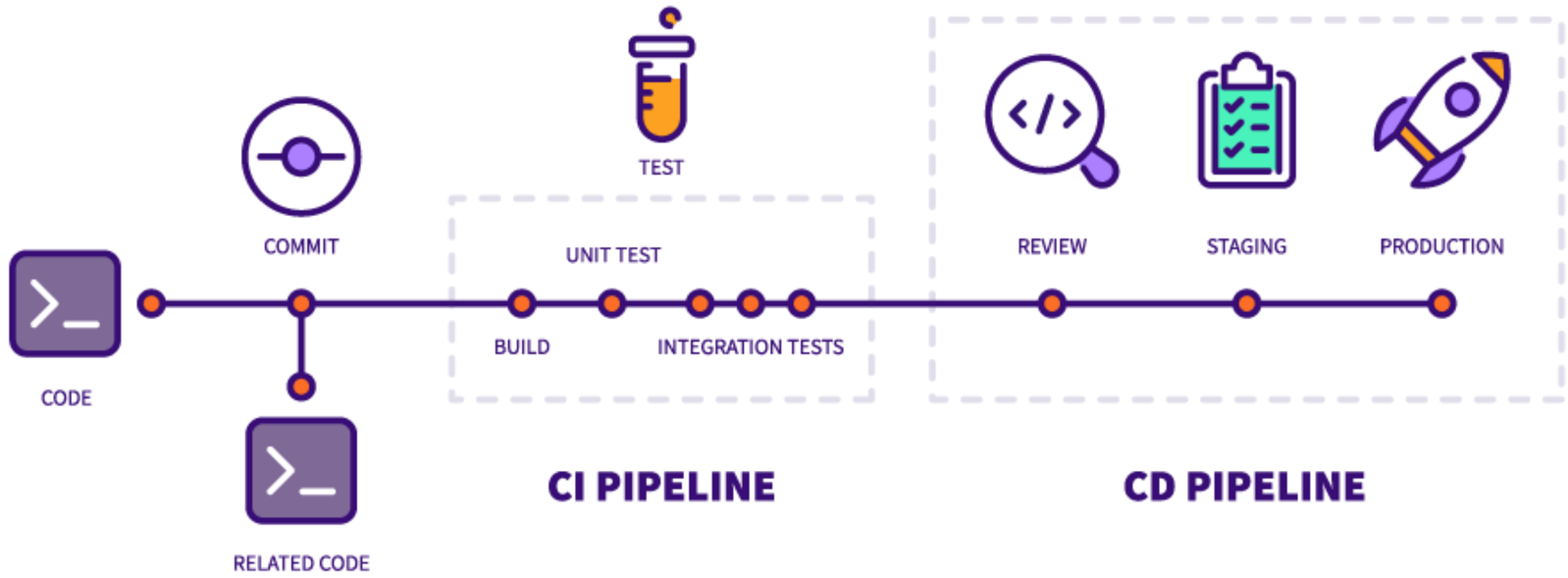
02 Pipelines implementation

03 Automation tests setup

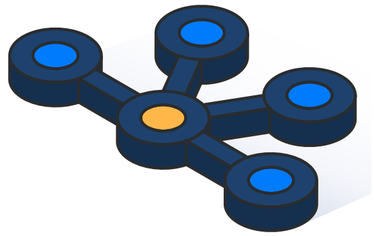
04 Infrastracture as Code implementation

05 Automatic deployment

06 Environment monitoring



Infrastructure as Code



Pattern advantages

- Cost reduction in terms of people and effort, meaning that by removing the manual activities, people are able to refocus their efforts on other enterprise tasks
- Infrastructure automation enables speed through faster infrastructure configuration and aims at providing visibility to help other teams across the enterprise work quickly and more efficiently.
- Automation removes the risk associated with human error, like manual misconfiguration; removing this can decrease downtime and increase reliability.

Deployment model

- public cloud
- private cloud
- hybrid cloud
- on-prem
- SaaS, PaaS

Architecture

- Ready to cloud deployment verification
- Service mapping
- Cloud native services usage
- Components adjustment

Automation

- automatic infrastructure creation
- pull, plan, apply
- run from pipeline
- multiple environments (dev, stage, prod)

Tools & Standards

- Terraform
- Ansible
- Chef
- Puppet
- Saltstack

Software adaptation

Review & Compliance

Conducting an audit on the basis of the technical documentation of the project, as well as code analysis in terms of identifying the real architecture is the first step to migration to the cloud.

Containerization

Docker image containerisation is the basis for automatic deployment and management your services using the most popular orchestrators such as Kubernetes, OpenShift, and more.

Adjustments

In the case of migration of an on-prem solution to the cloud, it is required to adapt the existing solution to the requirements of the cloud in technical terms, e.g. the use of native cloud services, but also business services, e.g. implementation of multitenancy, etc.

Configuration

The configuration of the solution is the next stage of implementation. At this stage, you need to configure the native services as well as the website that uses them. It is also the configuration of the security and network layer as well as other operational configuration.

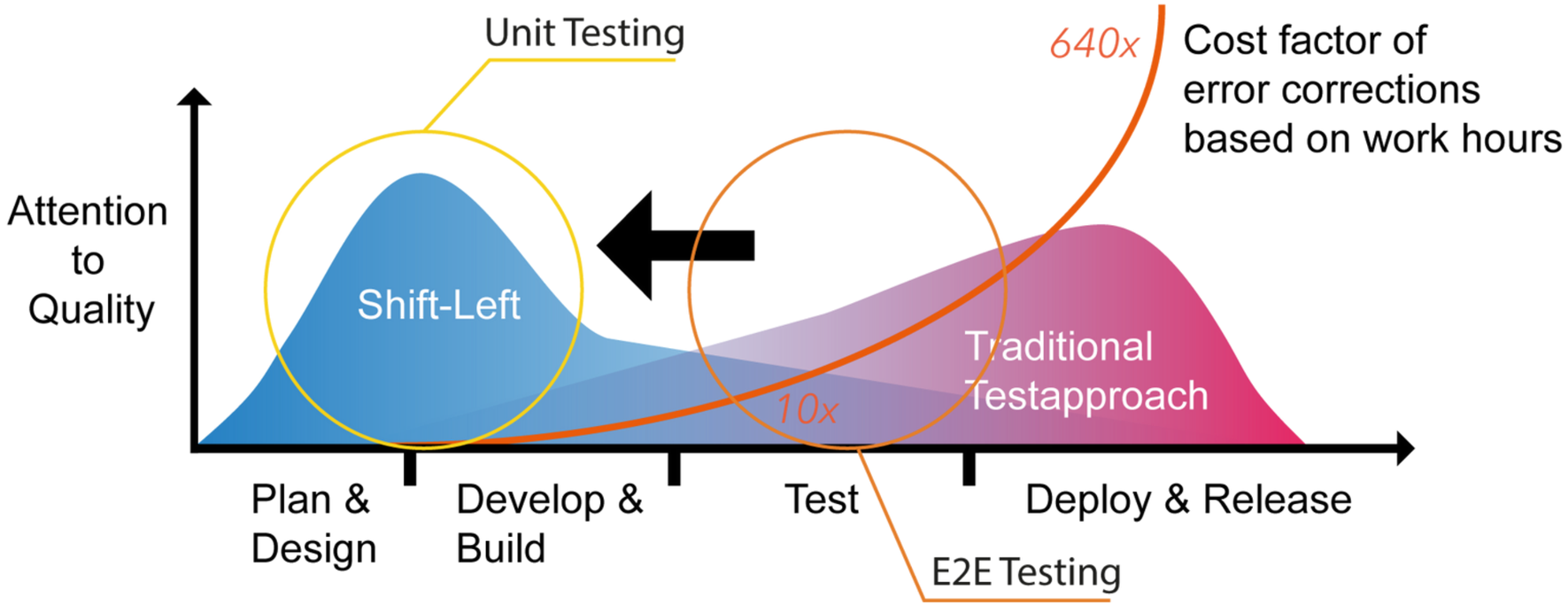
Tests automation

When implementing a solution to the cloud, it is worth taking care of test automation so that the tests are performed fully automatically during the pipeline run.
To ensure this, appropriate tools must be implemented and the current tests adjusted at different levels.

Deployment

Fully automatic deployment saves time and reduces the risk of human mistakes. Deployment is the last step in the pipeline run. It can be triggered differently depending on the type of environment. A well-functioning pipeline process means implementing changes to production in less than one hour.

Shift-left testing



Tests automation rules

- 100% stability
- 100% repeatability
- No nightly builds

Test automation tools

- Technology dependent unit tests
- TestContainers for integration tests
- Cypress for E2E tests

Test automation hierarchy

- Unit tests
- Integration tests
- E2E tests

Continuous Monitoring

Risk management

According to (ISC)² the Real-time (or near real-time) risk management cannot be fully achieved without continuous control monitoring using automated tools. Using automated tools, organizations can identify when the system is not in the desired state to meet security and privacy requirements and respond appropriately to maintain the security and privacy posture of the system. Continuous monitoring identifies undiscovered system components, misconfigurations, vulnerabilities, and unauthorized changes, all of which can potentially expose organizations to increased risk if not addressed

Tools

- Prometheus & Grafana
- AWS CloudWatch & X-Ray
- Splunk
- AppDynamic
- Dynatrace

Benefits

- Increase value through improved security and privacy controls.
- Accelerate reporting to support more rapid decision making and business improvement.
- Detect exceptions in real time to enable real-time responses.
- Reduce — and ultimately minimize — ongoing compliance costs.
- Replace manual preventative controls with automated detective controls.
- Establish a more automated, risk-based control environment with lower costs.
- Heighten competitive advantage and increase value to stakeholders.

"THE MOST POWERFUL TOOL WE HAVE AS DEVELOPERS IS AUTOMATION." — SCOTT HANSELMAN

DevOps Stack

The automation process requires the use of comprehensive knowledge and tools

01 **CI/CD: GitLab, TeamCity, Jenkins, Bambo**

02 **IaC: Terraform, Ansible, CloudFormation**

03 **Public Native Cloud: AWS, Azure, GCP, OCI**

04 **Private Cloud & on-premises**

05 **Orchestrators: Kubernetes, OpenShift, ECS**

06 **Shift-left testing: Cypress, TestContainers**

07 **Languages: Shell, Java, Node.js, Python**

Software delivery performance

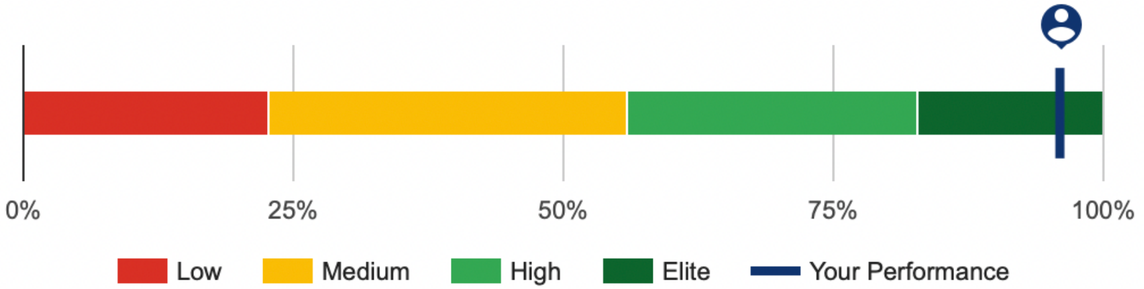
Google Cloud

according to Google DORA

Your performance:

Elite

You're performing better than 96% of State of DevOps Survey respondents.



01 Deployment frequency

02 Lead time for changes

03 Time to restore service

04 Change fail rate

DORA Elite aspects

Deployment frequency

For the primary application or service you work on, how often does your organization deploy code to production or release it to users?

On demand

Lead time for changes

For the primary application or service you work on, what is your lead time for changes (that is, how long does it take to go from code committed to code successfully running in production)?

Less than one day

Time to restore service

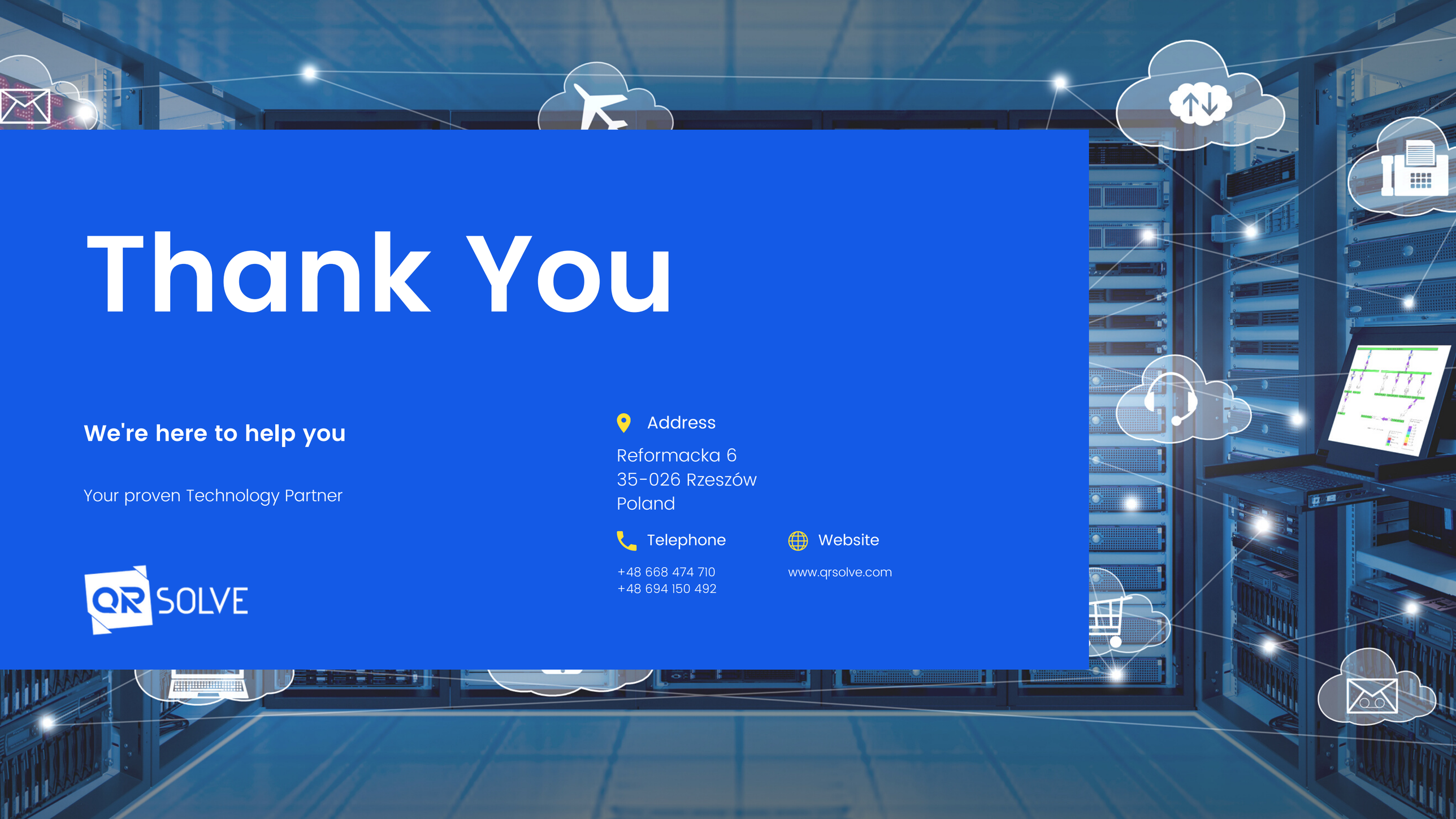
For the primary application or service you work on, how long does it generally take to restore service when a service incident or a defect that impacts users occurs?

Less than one hour

Change fail rate

For the primary application or service you work on, what percentage of changes to production or released to users result in degraded service and subsequently require remediation?

0–15%



Thank You

We're here to help you

Your proven Technology Partner

QR SOLVE

Address

Reformacka 6
35-026 Rzeszów
Poland

Telephone

+48 668 474 710
+48 694 150 492

Website

www.qrsolve.com