Information Security Guardrails

Version 1.0 February 2021

A collaborative effort between

to promote and foster security capabilities within financial service ecosystems.

Contents

Introduction

If you use cloud-based technology and you want to do business with any reputable company (think Financial Services, Healthcare, Utilities, Energy, etc) then you need to seriously consider your approach to cyber security.

While technology's shift towards cloud services has brought tremendous change to the security industry, the core principles that underpin technology security (i.e. why we have security controls in the first place) have not changed.

The shift has challenged *how* to execute traditional security models, *how* to protect information and *how* to defend against threats, but it has not changed *why* we do these things.

This creates a unique opportunity to define and embed new security models, built from the ground up and purposefully designed to work across cloud native and traditional on-premise technology environments. No more trying to retrofit security controls on top of legacy environments.

The cloud has also driven the expansion of security capabilities. The old security mantra of "the internet is bad" now actively prevents the adoption of best in breed security capabilities; companies must embrace cloud based security technologies to remain both relevant and safe.

If you're a cloud native organisation and you want to do business with large institutions, you need to embed security into the way you operate, in an enforced manner.

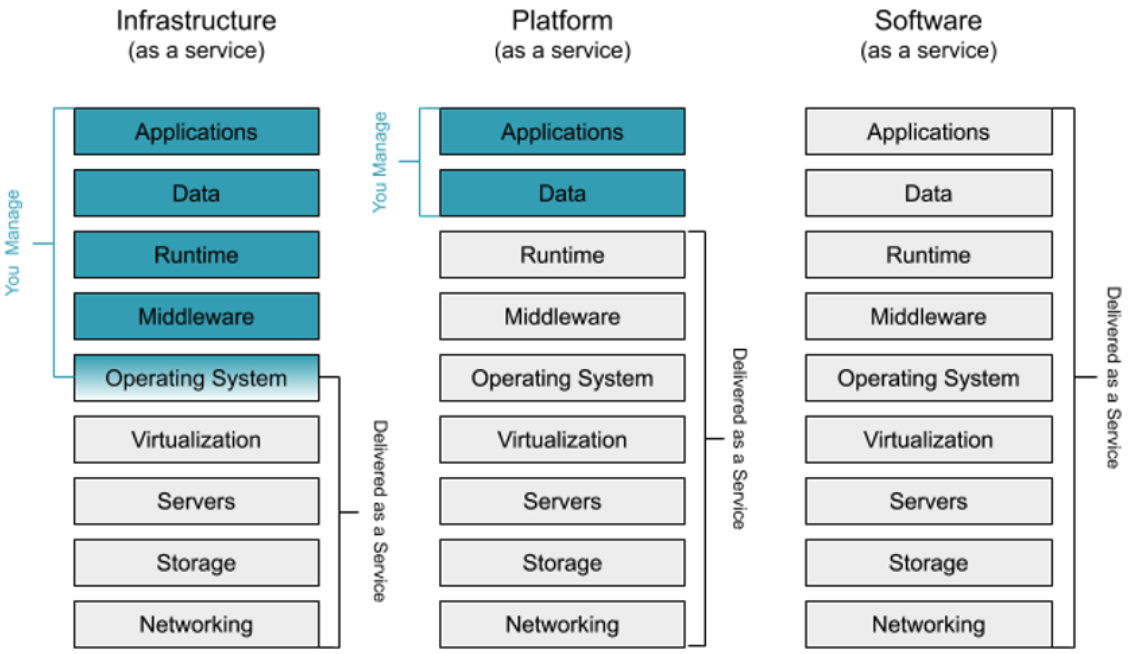
How to think about security

Trust is paramount and one way to earn and keep it is to ensure you create and maintain high security standards.

As we noted earlier, the core principles of technology security have not changed. Controls must be in place to mitigate and manage the risk of negative outcomes in relation to your operating environment, including the technology being used. These controls must be proportionate in the context of your business.

The operating concepts of "People, Process and Technology" still apply. The security concepts of "Confidentiality, Availability and Integrity" still apply. How you define and execute controls in relation to them is what may differ.

The concept of cloud computing plays host to many definitions but regardless of this, whenever any company buys a cloud service, they must understand what they must manage vs what is being managed for them. The U.S Department of Commerce's National Institute of Standards and Technology (NIST) [see NIST's definition of cloud] has a diagram that illustrates this well:



The use of cloud services requires reliance on cloud vendors so operational risks associated with vendor management must be managed appropriately. You are choosing to give up physical control of your data centres and various elements of technology management, from infrastructure through to software, in order to benefit from the advanced capabilities of institutions who specialise in this area.

This change in model transfers where the appropriate control points are in relation to the security of your environment, along with how to execute them. This type of outsourcing **does not outsource the risk itself**. The risk is still yours to manage and the responsibility is on you to ensure you are comfortable that your security standards are maintained. Seek to actively prevent both external threats and internal mistakes while you run and grow your business.

The technology used in your environment facilitates different functions. Evaluate and categorise those functions in alignment with Confidentiality, Integrity and Availability principles to determine what controls need to be put in place. Use Technology to streamline security Processes and help People manage security to the level required of a reputable institution that handles sensitive information.

Summary

We believe that keeping it simple is the key. A lot of security and compliance can be overwhelming or off putting because it feels “too technical” or nuanced. We’ve designed our 8 Categories to combat this by renaming core security principles using plain English to ensure you understand why their underpinning Guardrails are important.

We hope this helps you secure your environment so your users can be confident that your technology is fit for their financial information.

The Control Categories & Guardrails

In order to achieve our security goals we developed a model that categorises key control areas and attaches underlying principles, called Guardrails, to those categories that need to be met in some way.

The Guardrails are a Security Baseline for younger, cloud native companies that want to connect with reputable long-standing institutions.

Secure the Information

- All information at rest must be encrypted to industry-tested and accepted standards.
- All information in transit must be encrypted to industry-tested and accepted standards.
- All information must be categorised in a way that identifies Sensitive (SPII) and Personally Identifiable Information (PII) information.
    - All Sensitive (SPII) information must be encrypted at the field level.
- All cloud storage options must be configured to Private by default. Configuring storage to Public must be done as an exception.
- Information categorisation and protection must be automated.
- Each system must be categorised in accordance with the type of information it handles. This should be kept as simple as possible, it's either confidential or it’s not.

Control Access

- All technology must be configured to adhere to the Principle of Least Privilege.
- Role based access must be implemented.
- All technology must have an owner assigned and responsible for access control.
- Access reviews must be completed by owners quarterly.
- Administrative/Root/Owner access rights to Critical Systems must only be provisioned on a per exception basis.
    - Where this type of access can be provisioned using a temporal option, this must be used.
- Access to systems must be managed centrally by the owner / administrator.
- Access to Critical Systems must be managed centrally by the DevOps team.
- 2 Factor or Oauth (with 2 factor) must be enforced for critical systems.
- Use of privileged access on a Critical System must have an associated access request record.
- All system access should be logged. In many cases a successful attack relies on starting with a low privileged user and escalating from there. Having logs is therefore vital for investigations in the event of an incident.

Secure the Environment

- All cloud services must undergo due diligence / risk assessment prior to being used.
- The internal network must use VPN/VPC technology to separate and protect internal environments.
- Critical Systems must only use appropriately certified cloud services.
- The internal network must use a Zero Trust security model; avoid fully “trusted zones”.
- Application firewalls must be in place.
- Appropriate traffic control must be in place.
- Company devices must be managed centrally with enforced security settings.
- Devices with access to the internal environment must have anti-virus software (where appropriate), be patched up to date, and have hard drive encryption.
- Servers & Containers must be patched and up-to-date with latest Long Term Support versions as new vulnerabilities become known.
- Ongoing vulnerability scans must be carried out.
- Environment separation must be in place (Production, Staging, Development, Sandbox etc).
- Configuration monitoring solutions should be in place.

Control Change

- All changes to applications must go through a centrally managed CI/CD pipeline.
- All images and libraries used must be centrally managed and internally approved.
  - New images must be signed using cryptographic signatures.
- All changes must be security scanned prior to deployment.
- All major releases must be pen tested by a 3rd party prior to release. Be ready to share results with customers.
- All changes must have a code review and approval by another developer .
- A Change Management process should be adhered too.
- An Incident Management and Response process must be in place.

Embed Resiliency

- The technology environment must have appropriate resilience built in, based on the value and criticality of the service[oi15] [NP16] .
- Load balancing must be in place to ensure the environment copes with changes in traffic volume, and component failure.
- A regular backup process must be executed to facilitate recoverability within allotted Service Level Agreements.
- Hot/Hot and High Availability environments are not a substitute for Backups, both must be in place.
- Business Continuity exercises must be conducted annually and include the Production environment.
- Recoverability via Backups must be tested annually.
- Incidents must be able to be raised manually when necessary.

Embed Monitoring and Forensics

- Environmental monitoring and associated event-based alerting must be in place.
- Alerting rules must be configurable and tuned over time.
    - This must be appropriately linked to the Incident Management process.
- Logging of key events and associated actions must be in place. Logging is crucial as it is the only visibility into the environment.
- Event threat detection must be in place for anomalous threats / emerging events.
- Endpoints must support being remotely investigated for forensic purposes.
- There must be a forensic capability in place in the event the manual investigation of an event is required.
    - This will include access to logs from the environment to help see the issue to resolution.

Manage the Vendors

- All vendors must be assessed in accordance with due diligence requirements, including their ability to be used in the regulated financial services space, prior to use.
- Annual assessment of vendors must be conducted to ensure they remain fit for purposes.
- Regular monitoring of vendor performance must be conducted to look for early warning signs.
- Supplier contingency plans must be in place for vendors who support critical services.

Governance

- Appropriate Policies must be in place to manage the security of the environment, including but not limited to, information security, data management and privacy.
- Policies must be approved and owned by Senior Managers of the company.
- Security must be incorporated into the overall Risk Profile of the business.
- The company’s board must have visibility of the Operational Risk Profile.
- A regular Control Testing review must be in place and conducted.
