
7

Ursula Brennan: MoD reform, the view of the Permanent Under Secretary


48

Cougar 11: UK maritime capability in the Mediterranean


32

RAF's Reaper: The RPAS have a human side

DMJ Defence Management Journal

ISSUE 54 | Autumn 2011

Stepping up a gear

Collaboration fuels European defence

In association with:

DEFENCE INDUSTRIES Council

ADS www.adsgroup.org.uk

www.defencemanagement.com

Cover inspired by IVECO DEFENCE VEHICLES

Supported by Reply glue

PS analysis•opinion•debate

Cloud control

As data services and technology evolve, careful steps must be taken to ensure that integration and security are not compromised, says Glue Reply's Jason Hill…

The adoption of Cloud defence is just beginning. Cloud is a computing paradigm that delivers services via the internet. Information security is essential to any Cloud initiative and should not be viewed as a necessary evil nor simply a firewall issue. When information security goes bad, it has a big impact on business processes and operations. This risk is not solely related to the Cloud paradigm, but is related to the way the information is consumed across the defence process.

The Cloud value case is to reduce the cost of IT estates, but there is a risk that this cost will reappear in the integration or security layers as compliance costs increase and integration becomes more complex. Moreover, the cost may be felt in time as projects are delayed due to the paradigm shift in Cloud, integration and security.

Integration is the key IT enabler, connecting all areas of defence, its forces, suppliers and partners. With more data, functions and operations in deployed and non-deployed environments, the understanding of the 'business information' flows is a core capability in reducing cost and delivering effect. The main issues include:

- Decentralised security: applications and information are outside of the traditional firewall. Information accessed by means other than the application user interface must be secure;
- Unfixed location: the information resides on a virtualised environment. The provider can choose to upgrade and replace physical and virtual machines at will. Endpoint configuration must be flexible and dynamic;
- Business processes: are now codified in applications within and without the user's control. The Software as a Service (SaaS) provider[1] will have exposed only a limited number of standard entry and exit points for information. The cost of integration and process support will increase where bespoke touch-points are required;
- Scope of jurisdiction: data residence. Data export regulations have become more prevalent with the uptake of business process outsourcing and Cloud, particularly with SaaS. The location of the SaaS platform may be one thing, but tracking and securing 'in transit data' as part of an integrated business process is another. Understanding the 'security risk' of Cloud integration is a must: treating 'interfaces' as business services with active policy management can help provide the requisite assurance and transactional visibility;

> 'Integration is the key IT enabler, connecting all areas of defence, its forces, suppliers and partners.'

- Regulatory Compliance: legislation for PCI, FSA, DPA and NAO on the storage and provision of classified information relating is on the increase. Understanding 'who' and 'where' the user's data is controlled as part of compliance is a must;
- Speed and volume: defence has complex needs for its information. These needs are supported through different integration profiles. Establishing how high volumes and/or low latency consumption of off-premise data can be achieved through integration patterns is one way to avoid gridlock;
- Exit planning: today's buzz is Cloud, but what, as with some major outsourcing deals, does the 'customer' need to bring 'IT' back on-premise. Protecting and understanding the transactional boundaries of business applications and services can help avoid long and costly 're-integration' programmes.

If integration and security are to be done well (regardless of Cloud), upfront architecture, design and planning coupled with strong through-life governance are a prerequisite. The question of Cloud computing in defence is one of 'when, not if'. Understanding how to provide and consume data and information in Cloud and non-Cloud environments starts with sound architectures and results in slick and secure integration.

[1] An OEM contractor, government department or external vendor

Jason Hill
Partner
Glue Reply
Tel: +44 (0)1628 481553
k.couchman@replyltd.co.uk
www.gluereply.eu