Information Security – Musketeer Platform

ALL of your Information Security DATA in ONE place

What is Information Security?

Information security (IS) is designed to protect the confidentiality, integrity and availability of valuable data from those with malicious intentions and from accidental damage or disclosure.

Significant operational losses through online, internet and network fraud are real threats in today's digital society, highlighting the importance of maintaining the security and protection of your business, client and customer personal information.

The primary objectives of an information security program are to:

- **Increase confidence** over the availability of your data and related facilities through our business continuity module.
- Ensure the integrity of your data and information by providing **appropriate access** to systems and data with our RBAC access and review module.
- Manage and monitor **confidentiality by simplifying your information security management, oversight and reporting through effective configuration data base management and information risk management with our Information Security dashboard.**

Musketeer - The Information Security Platform

The primary focus of the IS platform is to manage all Information Security data in one place. This includes the following areas:

- All aspects of information security
- Help desk
- IS incident register and life-cycle management
- IS support and resource management
- IS access management
- Multi-platform mobile tools for IS related activities
- IS policy and procedure portal
- IS risk surveys
- Third party IS risk management
- IS assurance reviews
- IS SIEM Management
- IS Projects management
- IS data centre management
- Web Portal for call logging, reporting and supplier access
- Business intelligence reporting tools

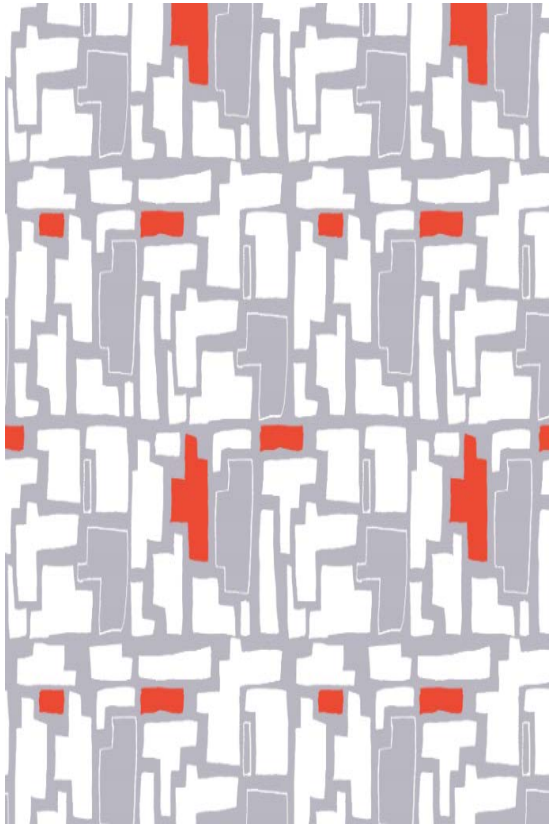
We achieve these through the implementation of a solution based on the immediate areas of concern, risk or loss. Our focus is on matching the implementation and delivery to your environment, capacity and people. Note that this is not intended to replace some of the specialized IS tools, we integrate with these to bring in the data as appropriate.

What are the benefits of Musketeer ISP?

Musketeer ISP delivers:

- ✓ Information Security operational excellence
- ✓ Cost certainty
- ✓ Risk reduction
- ✓ Enhanced and meaningful reporting
- ✓ Sustainability advances
- ✓ Business performance improvements
- ✓ Centralised store of all information assets
- ✓ Build rich and rewarding relationships with your suppliers
- ✓ Reduce security incidents
- ✓ Eliminate business disruptions
- ✓ Deliver consistent information security management processes and workflow
- ✓ Integration with existing solutions
- ✓ Automation of common and routine activities
- ✓ Support decision making and accountability
- ✓ Provide evidence of regulatory compliance
- ✓ Help build an effective and IS risk aware workforce

Musketeer ISP - Our Information Security Platform



Musketeer ISP is a tool that allows you to manage your corporate information assets globally. All related aspects of Information Security are now on a single platform. Musketeer ISP provides your CIO Executive, Information Security management team with an accurate IS inventory and management tool, designed to make managing the security of all information assets simple and effective.

You can realise the following benefits:

> ***Cost reduction*** **by eliminating the need for multiple solutions,**
>
> ***Product*** **enhancement by leveraging the solution for all information assets and your corporate physical assets,**
>
> ***Risk reduction*** **by tracking and monitoring Information Security from a single data source.**

Musketeer ISP provides you and your executive with online access to information about your information security assets. It is a one-stop management and planning tool for ongoing daily management and strategic planning for your corporate information assets. Musketeer ISP is an online, real-time web application designed to manage and support collaborative development, review, approval, and the co-ordination of all information security management services and activities.

All organisations today must take a holistic approach to cyber security to help prevent, detect and respond to advanced and evolving threats.

and respond to advanced and evolving threats.

Information Security Governance

Information Security governance addresses all aspects of the management and oversight of Information Security throughout your organisation. The complexity and potential impact on all organisations make Information Security a board level agenda item, requiring enhanced overall governance and oversight.

The IS governance model provides direction and oversight through the Information Security policy and procedures, Risk management, roles and responsibilities, awareness training and the management of KPIS and metrics. There is a direct relationship that is created with all critical aspects of the Board oversight too, allowing a single view across the full range of all IS.

IS policy and procedures must be up to date, provide detailed guidance and support decision making to meet your Information Security goals. Our Policy and Procedure module allows you to keep all policy and related procedures up to date, and linked to the

How enhanced IS Governance can help you

- ✓ Single source of IS information
- ✓ Enhancing Information Security as a board level agenda item
- ✓ Improving understanding and ownership for IS.
- ✓ Enabling direction and oversight
- ✓ Published Information Security policy and procedures,
- ✓ Support decision making to meet your Information Security Goals
- ✓ Linking IS to the IT department
- ✓ Supporting your executive committees' decision making.

How enhanced IS Access can help you

- ✓ Single source of IS information
- ✓ Replace multiple access tools and systems
- ✓ Prevent toxic combinations
- ✓ Improved oversight of who has what level of access
- ✓ Enforce principle of least access
- ✓ Automate UER assessments
- ✓ Maximise coverage
- ✓ Demonstrate accountability
- ✓ Reduce incidents
- ✓ Supporting your executive committees' decision making.

IS application and access management

All organisations today have several applications in production that manage the operations, and provide the foundation of the day to day operations. A key requirement that most companies will require is the principle of least privilege, so that access to applications and data is restricted to those who require it. This has proven to be complex, time consuming and very difficult to implement in large organisations.

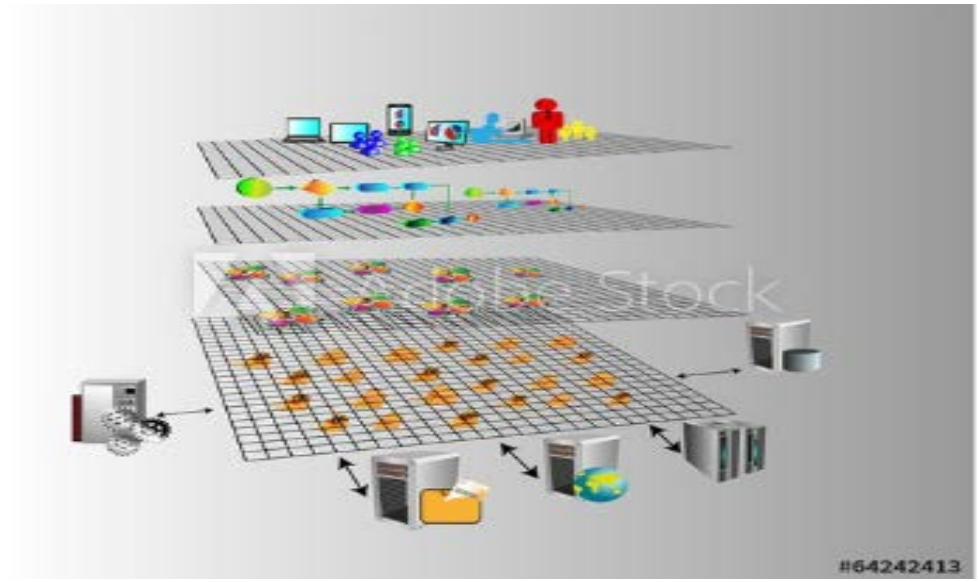
Our approach is to address, at a minimum, the following components:

- Application Ownership
- Role based access control and provisioning (refer to separate module)
- Recertification
- Privileged user access
- Provision, review and revocation of access, and employee screening
- Remote access

The holistic approach adopted by this module provides the solution for many large organisations. Whilst working with the current solutions, we deliver a comprehensive approach to driving ownership and accountability for Application and Information owners, Line Managers and the HR team.

How enhanced IS Architecture can help you

- ✓ Single source of IS information
- ✓ Oversight of multiple projects and work streams
- ✓ Encourages policy compliance
- ✓ Measures policy compliance
- ✓ Enables risk-based decision making
- ✓ Creates unified approach to enterprise modelling
- ✓ Supports re-use of artefacts
- ✓ Provides a common repository and control
- ✓ Supporting your executive committees' decision making.



IS architecture

The typical organisation will have many IT projects and initiatives on the go, with many of them requiring direct support, and sometimes intervention, to make sure that they include security controls to ensure that the information assets are secure and safeguarded.

The focus of the IS architecture team is to set the Information Security standards in line with your IT functions (refer to separate ITIL module) and make sure that the standards are applied across development, infrastructure, networks and the change management operations.

A large proportion of the work carried out requires the management of the policies and standards required over the many IT areas, requiring the use of the Policies and Standards module. The work is typically project based, requiring the use of the Project portfolio and management modules to provide oversight of the activities being carried out.

Musketeer makes managing security across multiple projects and ensuring compliance with policy simple by pulling together policy and project information.

IS Security Operations

The IS Security Operations team are responsible for the technical operations for Information Security. This is a critical component of the Information Security defence as they provide the perimeter protection and prevention tools for keeping the operations secure. Our solution provides a common repository to store and track all data and projects relating to the IS Security Operations to support the multiple specialized tools that are currently used.

Some of the core elements that are included are:

- SIEM
- Malware
- Penetration testing
- Data Leakage
- Media management
- Data transfers
- Threat management

The solution provides several APIs to many of the current offerings in the market, and provides a comprehensive and consolidated view of all events.

How enhanced IS Sec Ops can help you

- ✓ Single source of IS information
- ✓ Oversight of all Security Operations activities
- ✓ Enhanced decision making enabled by timely information
- ✓ Alert management
- ✓ Trending and analytics
- ✓ Action management
- ✓ Common approach to setting priority
- ✓ Accountability
- ✓ Workflow to manage events
- ✓ Forward looking threat assessments
- ✓ Supporting your executive committees' decision making.

Information Security Help Desk

Our customers, including internal and external stakeholders, require support on an ongoing basis to deal with a multitude of Information Security requests and issues. The stakeholders also require several routine requests, based on the scope and services provided by the Information Security team.

As your typical Information Security team will need to respond to hundreds of IS support, queries, potential IS incidents and related urgent issues each year, our Information Security Service desk module must establish and develop a reputation for effective and quick responses to make sure that the people are protected and the information assets are SECURE.

This module is based on the generic service desk module, with specific enhancements that are required for the Information Security team.

How a IS Help Desk can help you

- ✓ Single source of IS information
- ✓ Common logging of IS incidents
- ✓ Centralised KPIs
- ✓ Tracking of actions and outcomes
- ✓ Easy identification of problem areas and units
- ✓ Tracking of time and effort on issues
- ✓ Trending and reporting
- ✓ Escalation links where required
- ✓ Supporting your executive committees' decision making.

How CSCs can help you

- ✓ Single source of IS information
- ✓ Validation against a recognised international standard (NIST CSC)
- ✓ Common view of critical KPIs
- ✓ Formal feedback to executives
- ✓ Early warning mechanisms
- ✓ Reduced exposures
- ✓ Technical coverage measured and reported
- ✓ Reduced impact of litigation
- ✓ Supporting your executive committees' decision making.

Critical Security Controls

The Critical Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. Critical Security Controls for cyber defence are a baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence.

Cyber threats make the headlines on a regular basis. According to the 2016 Cost of Data Breach Study (US) from the Ponemon Institute, the average cost of a data breach in the UK is £2.53 million, a 6.5% increase in total cost over 2 years.

The 20 controls focus on technical measures and activities, with the primary goal of helping organisations prioritise their efforts to defend against the current most common and damaging computer and network attacks. A principle benefit of the Controls is that they prioritize and focus a smaller number of actions with high pay-off results.

IT Risk Management

How enhanced IT Risk can help you

- ✓ Single source of IS information
- ✓ Common risk platform
- ✓ Generic rating solution
- ✓ View of mitigation and progress
- ✓ Extended scenario planning
- ✓ Mix of what has gone wrong with what could
- ✓ Supporting your executive committees' decision making.

The Information Security team plays a vital role in the management of IT risk. Using the Risk Management module, we allow the tracking of all IS related risks, covering events that have occurred and their closure, potential events that may occur and the mitigation actions required to address them, and scenario planning to assist in mapping out the IS focus areas and allocation of resources.

We apply the generic risk management approach, using a common set of assessment criteria (impact, likelihood) that provides the risk owners with a common view of the IS activity, as well as providing the risk heat maps and other relevant risk management processes.

The management of the risk for Information Security is carried out with the IT teams, and provides a core part of the overall risk landscape.

Information Security Assurance

The Information Security assurance approach has provided a complex set of requirements that are difficult to address, given the breadth and scope of potential issues that need to be addressed.

Whilst our approach provides the management of all IS assurance activities (projects, findings, ratings, red flags, business area assessment scores), one of our flagship products is the monitoring of all externally related traffic from your company portals. We provide a comprehensive view, either as a once off assessment or an ongoing review, we can give you the comfort and peace of mind that your external traffic is secure, and that potential data loss events are detected and can be closed.

This uses the IP logs of all external traffic, and using a sophisticated set of algorithms and unique routines, provides a comprehensive, risk based view of actual activity on your network. There is a large range of risks covered – these are prioritised and summarised in a comprehensive audit report.

How enhanced IS Assurance can help you

- ✓ Single source of IS information
- ✓ Improved coverage
- ✓ Ability to demonstrate resource requirements
- ✓ Direct alignment to policy, risk and incidents
- ✓ Aligned with accountability and ownership
- ✓ Common project and reporting platform
- ✓ Tracking findings and recommendations
- ✓ Support for creating preventative actions
- ✓ Supporting your executive committees' decision making.

Service Delivery Options

We have several options for implementation, which are wholly dependent on your infrastructure, IT environment and preferred IT delivery model.

Our SaaS solutions give you 24/7 access to your system from anywhere with an internet connection. SaaS offers a number of benefits, including: Complete security for your data; Reduced upfront costs; Quick implementation; and potentially Lower total costs of ownership

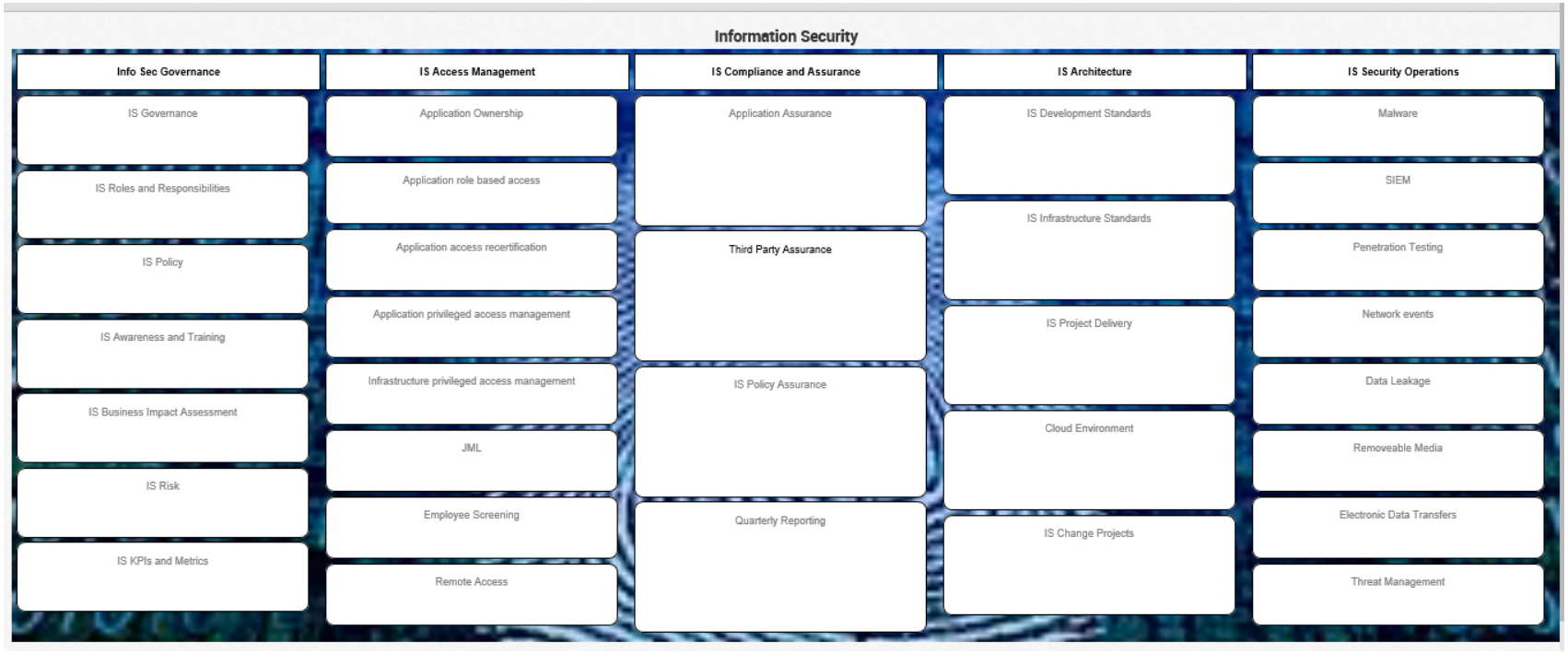
Our hosting options include dedicated and multi-tenanted cloud service or full disaster recovery. So whether you are looking for a cost effective SaaS solution or a premium service, we have a range of solutions on offer to perfectly suit your business.

Easy Setup

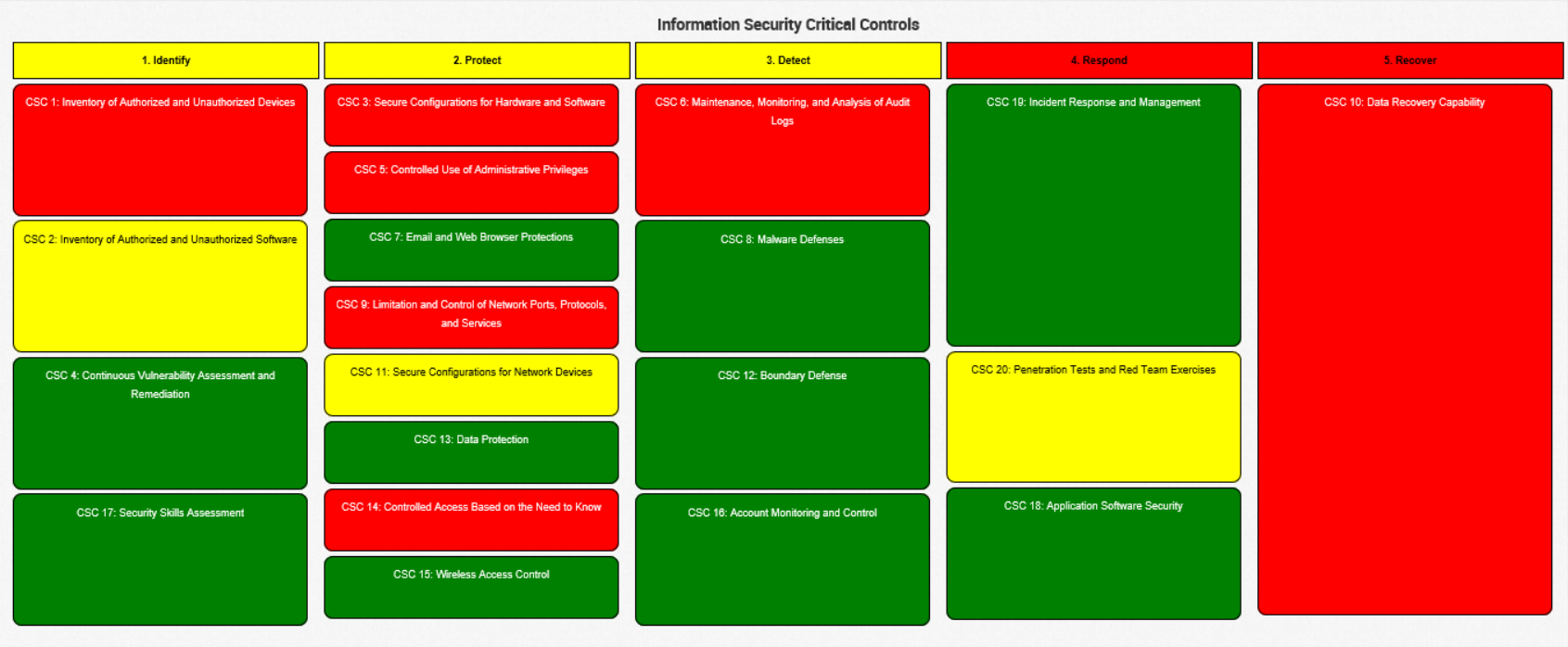
User Friendly

Access Anywhere

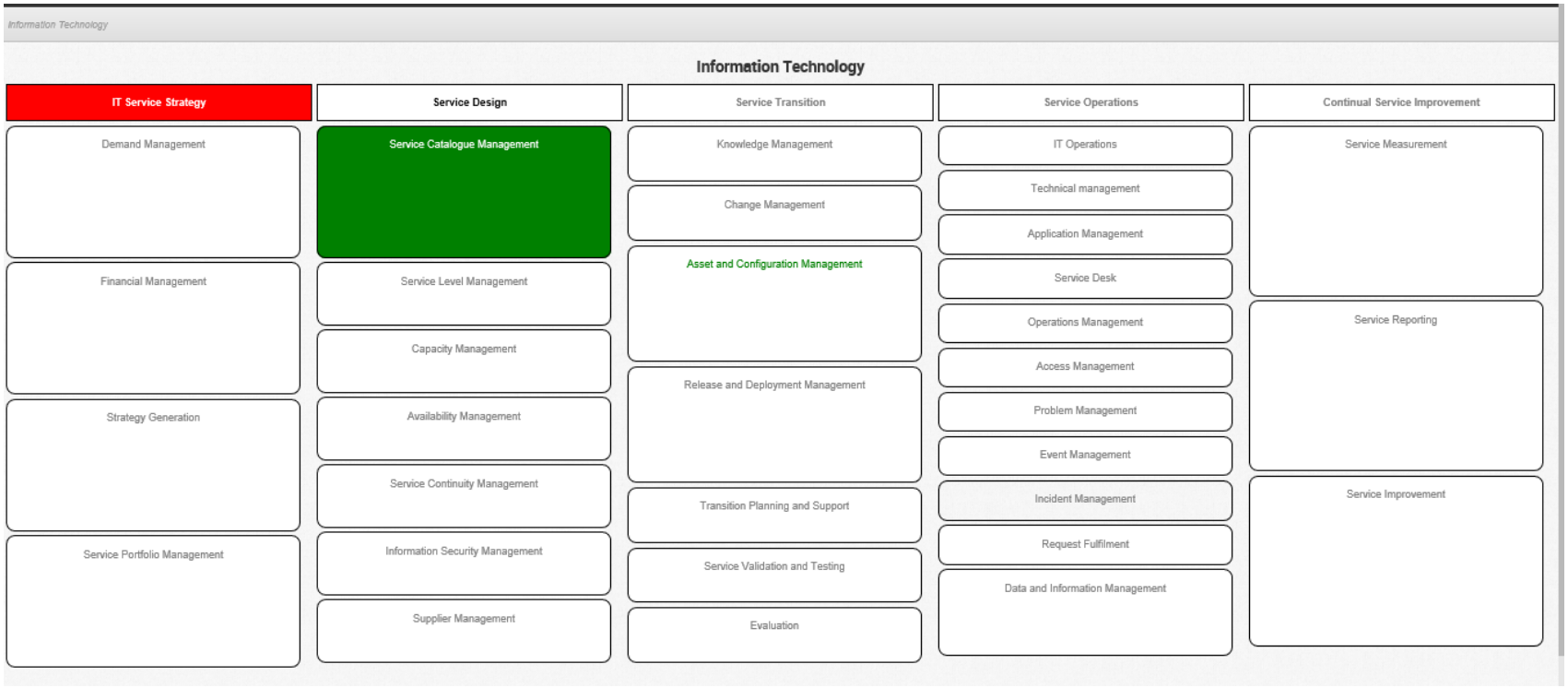
Sample Client IS Dashboard



Sample Client Top 20 Cyber Controls Dashboard



Sample Client IT Dashboard



End