# Information Security Optimization

Kurt Salmon

## Client challenges

**Continuous high profile incidents of organized hacking activities against corporations highlight the importance of protecting organizations against risk, while enabling them to continue to do business effectively and efficiently.**
**A company's inability to comply with security standards is generally due to the inefficiency of their processes and not necessarily their tools.**

CIOs face a number of critical questions:

- Are my IT Security resources working efficiently to address the real risks of the company?
- How many employees are performing security functions within my organization? What are they spending their time on?
- Why is our organization failing audits when we have so many skilled personnel?
- Are these security processes really addressing risks or simply quashing productivity for no other reason than 'this is the procedure we have always had in place"?
- Do we require more consistent security processes and, if so, how do we go about defining, justifying and implementing them?


Please contact:

**Jeremy Cicurel**
*Practice Director*
*CIO Advisory*
jeremy.cicurel@kurtsalmon.com

**Follow us on Twitter:** @KurtSalmonCIONA

www.kurtsalmon.com




## Kurt Salmon solutions

**While traditional cost benefit analysis is useful for optimizing resources, an IT Security group must consider additional risk-related parameters that transcend costs to create a lifecycle approach for efficient management of the IT Security organization:**

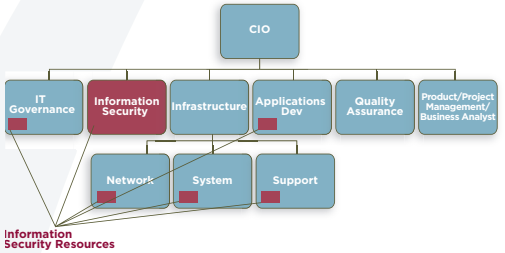
**Optimize and Streamline Processes** with the highest value to reduce internal risks and external threats
**Develop Key Performance Indicators** to determine its effectiveness within the overall enterprise
**Establish Key Risk Indicators** with the organization to assess risk appetite

Kurt Salmon provides clients with immediate process improvement in seven proven steps by:

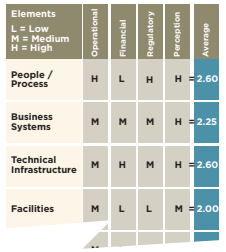
1. *Mapping existing processes*
2. *Rating the maturity of the processes*
3. *Prioritizing and optimizing processes*
4. *Developing a target process improvement roadmap*
5. *Defining a lifecycle and aligning it to the overall IT lifecycle*
6. *Implementing a security dashboard for Key Performance Indicators (KPI) and Key Risk Indicators (KRI)*
7. *Increasing the level of security with ongoing maintenance and continuous improvements*

## Illustrative deliverables

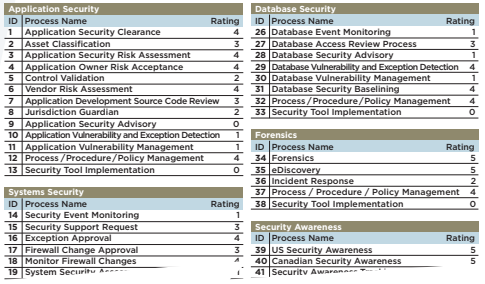
### *Mapping of Security Resources*




### *Risk Assessment*




### *Security Process Rating*



| Application Security | | |
|---|---|---|
| ID | Process Name | Rating |
| 1 | Application Security Clearance | 4 |
| 2 | Asset Classification | 3 |
| 3 | Application Security Risk Assessment | 4 |
| 4 | Application Owner Risk Acceptance | 4 |
| 5 | Control Validation | 2 |
| 6 | Vendor Risk Assessment | 4 |
| 7 | Application Development Source Code Review | 3 |
| 8 | Jurisdiction Guardian | 2 |
| 9 | Application Security Advisory | 0 |
| 10 | Application Vulnerability and Exception Detection | 1 |
| 11 | Application Vulnerability Management | 1 |
| 12 | Process / Procedure / Policy Management | 4 |
| 13 | Security Tool Implementation | 0 |

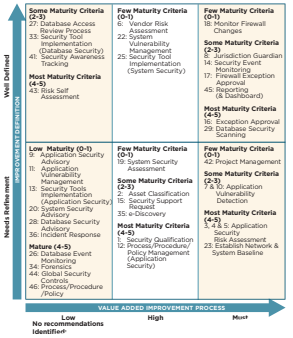
| Systems Security | | |
|---|---|---|
| ID | Process Name | Rating |
| 14 | Security Event Monitoring | 1 |
| 15 | Security Support Request | 3 |
| 16 | Exception Approval | 4 |
| 17 | Firewall Change Approval | 3 |
| 18 | Monitor Firewall Changes | 4 |
| 19 | System Security Approval | 1 |

| Database Security | | |
|---|---|---|
| ID | Process Name | Rating |
| 26 | Database Event Monitoring | 1 |
| 27 | Database Access Review Process | 3 |
| 28 | Database Security Advisory | 1 |
| 29 | Database Vulnerability and Exception Detection | 4 |
| 30 | Database Vulnerability Management | 1 |
| 31 | Database Security Baselining | 4 |
| 32 | Process / Procedure / Policy Management | 4 |
| 33 | Security Tool Implementation | 0 |

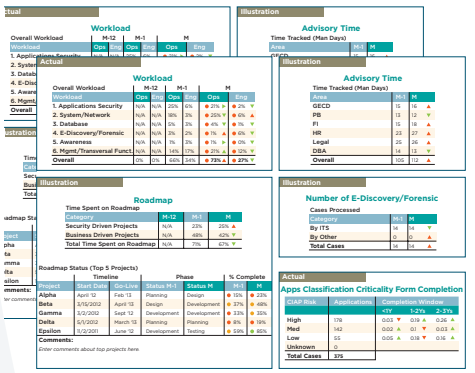
| Forensics | | |
|---|---|---|
| ID | Process Name | Rating |
| 34 | Forensics | 5 |
| 35 | eDiscovery | 5 |
| 36 | Incident Response | 2 |
| 37 | Process / Procedure / Policy Management | 4 |
| 38 | Security Tool Implementation | 0 |

| Security Awareness | | |
|---|---|---|
| ID | Process Name | Rating |
| 39 | US Security Awareness | 5 |
| 40 | Canadian Security Awareness | 5 |
| 41 | Security Awareness Training | 4 |

### *Process Improvement Matrix*




### *Key Performance & Risk Indicators Dashboard*




### *Security Lifecycle-Continuous Improvement Diagram*