Protecting Confidentiality, Integrity and Availability of sensitive data through Good Software Engineering Practice

ISACA Nordic Conference 7-8 April 2014
Norway, Oslo

Pouya Pourkomeylian Ph.D.
IT Compliance Director
pouya.pourkomeylian@molnlycke.com
+46739503619
My background

- **System Science** – Lund University - B.Sc. 1994 – Information Security
- **Informatics** – Lund University - M.Sc. 1995 – Information Security
- **Informatics** – Göteborg University - Ph.D. 1999-2002 (Industrial PhD program parallel with my AstraZeneca assignments – Software Engineering - Software Process Improvement)
- **University of Trollhättan and Uddevalla** – Lecturer 1995-1996
- **IT-University in Göteborg** - 2002-2006 – (Senior lecturer and guest researcher – Establishing the Software Engineering Program at the IT University in GBG, and teaching in Software Process and Quality Mgt - Evening activities)
- **Acando** – Senior Management Consultant – Oct 2011-2012
- **Möllycke Health Care** – IT Compliance Director and KAM for LR&QA – 2012 -
Protecting Information / Data

• Protecting information has been a challenge to deal with for a long time – At the same time if addressed correctly has the potential to offer competitive advantages

• Today, we all (as individuals, small, middle, large companies, and governments) in one or other way are vulnerable when it comes to lack of information/data “quality” and are also depended on data protection measures and controls.

• We can see different attempts in almost all organizations (from “just” a Policy in place towards implementing heavy technical Data Loss Prevention solutions). But the issue is still there

• In today's sociality, data protection is an open issue putting all of us on risk – The issue is multi dimensional, difficult to localize, easy to ignore, and almost impossible to mitigate totally
### Characteristics of Efficient Security Governance


<table>
<thead>
<tr>
<th>No</th>
<th>The Characteristics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An Enterprise-Wide Issue</td>
<td>The scope of the security work to cover the whole organization horizontally, vertically, and cross-functionally including people, products, processes, policies, procedures, systems, technologies, networks, and information.</td>
</tr>
<tr>
<td>2</td>
<td>Accountable Leaders</td>
<td>Executive management understands their accountability for information security. The senior managers to be engaged in the management and follow up of the information security efforts and support the work by financial resources, management, risk based policies, and annual reviews and audits. Business leaders understand and accept their responsibilities and ownership for information security risks and the associated assets, e.g. systems, networks, applications.</td>
</tr>
<tr>
<td>3</td>
<td>Viewed as business requirement</td>
<td>Security to be viewed as business requirement rather than an additional cost item.</td>
</tr>
<tr>
<td>4</td>
<td>Risk based</td>
<td>The level of security measures should be risk based.</td>
</tr>
<tr>
<td>5</td>
<td>Roles, Responsibilities, and Segregation of Duties</td>
<td>Clear definitions for roles and responsibilities that take into account segregation of duties, accountability, and risk management.</td>
</tr>
<tr>
<td>6</td>
<td>Addressed and Enforced in Policy</td>
<td>Information Security rules, and requirements are clearly defined in policies and implemented through procedures which are supported by trained people and technical solutions including controls and reporting structures.</td>
</tr>
<tr>
<td>7</td>
<td>Adequate Resources Committed</td>
<td>Trained and capable resources are available.</td>
</tr>
<tr>
<td>8</td>
<td>Staff Aware and Trained</td>
<td>Information security awareness level is in line with company’s security ambitions.</td>
</tr>
<tr>
<td>9</td>
<td>A Development Life Cycle Requirement</td>
<td>Information security requirements and rules are addressed through System Life Cycle processes</td>
</tr>
<tr>
<td>10</td>
<td>Planned, Managed, Measurable, and Measured</td>
<td>Information security efforts are planned and managed. Information security has measurable objectives and its performance is continuously measured.</td>
</tr>
<tr>
<td>11</td>
<td>Reviewed and Audited</td>
<td>Company’s risk and audit organizations are conducting regular reviews and audits on company’s information security efforts.</td>
</tr>
</tbody>
</table>

Medical Device Industry & IT Compliance?

To maintain the company’s License to Operate!

through

Protecting confidentiality, integrity, and availability of data, which if modified in an uncontrolled way might have risk impact on Patient Safety & Product Quality
Enforcing Software Engineering Discipline through Regulation in Pharma & Medical Device Industry

**FDA 21 CFR 820**
2. QMS
3. Design Controls
4. Document Controls
5. Purchasing Controls
6. Identification & Traceability
7. Production & process Controls
8. Acceptance Activities
9. Nonconforming Product
10. Corrective & preventive Action
11. Labeling & Packaging Control
12. Handling, Storage, Distribution, & Installation
13. Records
14. Servicing
15. Statistical Techniques

**FDA 21 CFR Part 11**
2. Electronic Records
3. Electronic Signatures

**Software Validation & Infrastructure Qualification**
- The Software is validated for its intended USE
- The Infrastructure is kept in a state of control using an infrastructure life cycle approach

**Supporting & Maintenance Organization**
- BCP, DRP, Access Control, Incident, Problem, Change, and Release Mgt
- Training
- Supporting & Maintenance Organization

**Establishing the Software Validation & Infrastructure Qualification Status once and maintain it through the System’s and the Infrastructures Life Span**

Diagram:
- Specifying the Infrastructure
  - IQ
  - OQ
  - Infrastructure Qualification Report
Regulation based V.S. Tool driven Data Protection Projects - Own experience

The Tool driven project – Conducting a PoC – Company A

- New R&D in India – IP to be protected from unauthorized eyes
- Guided by the tool
- Let’s assume a “policy” and play the game
- Protecting well the defined in scoped Data/Document within the Policy
- Reports on violations from the Policy caused by practitioners trying to do some none authorized actions
- Not Risk focus
- Need to do your “homework”
- Running a PoC project VS implanting such a concept in the context of a global organization
- This requires a clear and defined information governance structure

The Regulation driven project – An analysis on How to protect sensitive information – Company B

- Sensitive information should be protected from unauthorized eyes
- Forced to define What
- Not guided by the approach in defining the data Protection/Quality attribute
- “Interpretations” oriented – depended of one Key person
- Regulatory requirements were the ONLY “guiding principle”
- No interest in taking to account the risk factor in relation to protection and control
- Need to put the information protection efforts in a wider context than only regulatory requirements based
A usual day at work for many of us
Protecting Data – a multi dimensional issue

Do I have the “right” Focus?
- Which Data to protect? Classified information
- Which Data Quality Attributes are in focus for which Data? (Confidentiality, Integrity, Availability, etc.)
- Where does this Data exists? Data in motion, at end points, in rest?

Am I aware of the potential and actual Risks?
- What is the Total Risk Impact on losing Data?
- What is the level of Data Lost today?
- What is my Risk appetite?

Do I have the “right” level of Protection, where and when needed?
- What is the level of Protection today?
- Is the existing protection proportional to the level of risk I have?

Do I have the right level of Capabilities in place?
- What is the maturity level of my IS/IT processes?
- What is the level of knowledge and awareness of people?
- What is the level of Software Validation and Infrastructure Qualification in my organization?

Do I have the “right” level of Control, where and when needed?
- What is the level of Control in place today?
- Is the existing control(s) proportional to the level of risk I’m facing today?
A Maturity and Risk based Data Protection Journey

- Poor Risk Management
- Higher Cost
- Lower Efficiency
- Unstable Performance / Delivery

**The Maturity Journey**

**Level 1 - Ad Hoc**
- Process unpredictable, poorly controlled, and reactive

**Level 2 - Repeatable**
- Process characterize for some projects and is often reactive

**Level 3 - Defined & Agreed**
- Process characterize for Organization and is often proactive

**Level 4 - Quantitatively Managed**
- Process measured and controlled

**Level 5 - Optimized**
- Focus on continuous Process improvement

**Risks**
- Efficient Risk Management
- Lower Cost
- Higher Efficiency
- Sustainable Performance / Delivery

**Protection**

**Capabilities**

**Controls**
Balancing the efforts
A “FIT FOR YOU” Risk based approach

99% of the identified risks mitigated through protection measures

Automated Technical Protection Applied, e.g. DLP tools

99% Process optimization achieved
Continuous Improvement in place
Knowledge and awareness in place

99% of identified risks & applied measures are controlled
Automated Integrated Assurance Applied

Where are you today?

Where should you be?
AND
What should you do?

The “Art” in this context will be to set the level of Efforts based on your organizations tolerance for risk.

Risk Mgt maturity level
Protection maturity level
Control maturity level
Capability maturity level

Risk based approach cultivated
Total risk impact identified
Risk appetite defined and communicated
Risk based decision is applied

Risk Mgt process with connection to protection and control defined
Basic measures, what & how are documented
Protection for selected risky areas in place
Automated tools are optimizing the level of protection

Ad hoc “risk mgt” in some areas
“Gut feeling” based protections adopted by some people
Basic control routines in place for some areas
Automated tools are optimizing the level of integrated control and reporting on violations

No risk awareness
Basic control routines adopted by some people
“Gut feeling” based way of working
 Automatized tools

Knowledge and awareness in place
Defined processes in place
Defined way of working adopted and measured
Defined way of working optimized

Risk based approach cultivated
Total risk impact identified
Risk appetite defined and communicated
Risk based decision is applied

Where are you today?

Where should you be?
AND
What should you do?

The “Art” in this context will be to set the level of Efforts based on your organizations tolerance for risk.

Risk Mgt maturity level
Protection maturity level
Control maturity level
Capability maturity level

Risk based approach cultivated
Total risk impact identified
Risk appetite defined and communicated
Risk based decision is applied

Risk Mgt process with connection to protection and control defined
Basic measures, what & how are documented
Protection for selected risky areas in place
Automated tools are optimizing the level of protection

Ad hoc “risk mgt” in some areas
“Gut feeling” based protections adopted by some people
Basic control routines in place for some areas
Automated tools are optimizing the level of integrated control and reporting on violations

No risk awareness
Basic control routines adopted by some people
“Gut feeling” based way of working
 Automatized tools

Knowledge and awareness in place
Defined processes in place
Defined way of working adopted and measured
Defined way of working optimized

Risk based approach cultivated
Total risk impact identified
Risk appetite defined and communicated
Risk based decision is applied

Risk Mgt process with connection to protection and control defined
Basic measures, what & how are documented
Protection for selected risky areas in place
Automated tools are optimizing the level of protection

Ad hoc “risk mgt” in some areas
“Gut feeling” based protections adopted by some people
Basic control routines in place for some areas
Automated tools are optimizing the level of integrated control and reporting on violations

No risk awareness
Basic control routines adopted by some people
“Gut feeling” based way of working
 Automatized tools

Knowledge and awareness in place
Defined processes in place
Defined way of working adopted and measured
Defined way of working optimized

Risk based approach cultivated
Total risk impact identified
Risk appetite defined and communicated
Risk based decision is applied

Risk Mgt process with connection to protection and control defined
Basic measures, what & how are documented
Protection for selected risky areas in place
Automated tools are optimizing the level of protection

Ad hoc “risk mgt” in some areas
“Gut feeling” based protections adopted by some people
Basic control routines in place for some areas
Automated tools are optimizing the level of integrated control and reporting on violations

No risk awareness
Basic control routines adopted by some people
“Gut feeling” based way of working
 Automatized tools

Knowledge and awareness in place
Defined processes in place
Defined way of working adopted and measured
Defined way of working optimized

Risk based approach cultivated
Total risk impact identified
Risk appetite defined and communicated
Risk based decision is applied

Risk Mgt process with connection to protection and control defined
Basic measures, what & how are documented
Protection for selected risky areas in place
Automated tools are optimizing the level of protection

Ad hoc “risk mgt” in some areas
“Gut feeling” based protections adopted by some people
Basic control routines in place for some areas
Automated tools are optimizing the level of integrated control and reporting on violations

No risk awareness
Basic control routines adopted by some people
“Gut feeling” based way of working
 Automatized tools

Knowledge and awareness in place
Defined processes in place
Defined way of working adopted and measured
Defined way of working optimized
Lessons Learned - Before “jumping” into any “Data Protection” activities

2. Ensure that you have the “right” sponsor – Executive level – This is NOT a question to be owned by the CIO / Security Officer!
3. Find out Where are you today? Maturity level when it comes to Risk Mgt, Protection, Capabilities, and Controls.
4. Find out What to be protected, Where, & from Whom?
5. Find out which protection & control levels do you need for which type of information (e.g. Secret, Top Secret) in relation to the existing risks/threats?
6. Find out who is owning information and deciding on protection levels?
7. Define the organization’s Data protection Strategy based on a Maturity and Risk based approach – Where you should be
8. By this stage you’ve done your homework – the rest is “just” a matter of Project Planning, Execution, and Measuring effects
9. Go to your STCO get the resources and budget
10. Do it & make it a BAU
Thanks

Happy to take questions

So, where do you want to go?