Checking Assignments of Controls to Risks for Internal Control

Yasuhito Arimoto*
Yuji Watanabe**
Michiharu Kudoh**
Kokichi Futatsugi*

*: Japan Advanced Institute of Science and Technology
**: IBM Tokyo Research Laboratory
A process effected by an organization’s structure, work and authority flows, people and management information systems, designed to help the organization accomplish specific goals or objectives.

- by the Committee of Sponsoring Organizations of the Treadway Commission (COSO)

• Aims of Internal control
  – Efficacy and efficiency of the business
  – Trustworthiness of the financial reports
  – Compliance with applicable laws and regulations
Establishment of Law

• Sarbanes-Oxley Act (2002, US)
• Financial Instruments Exchange Law (2006, Japan)
  – Financial reporting
    • Evaluation of internal controls by management
    • Audit of the evaluation’s report by external auditor
Process of Financial Reporting
Documents of Internal Control

- Business workflows
- Risk and control matrices
  - Relations of risks and controls
- Business process narratives
  - Detailed information of business workflows
Evaluation

![Diagram showing evaluation process]

- Business process narrative
- Risk and control matrix
- Business workflow
- Decision-making Criteria
- Management

Evaluate
Aim

- Evaluation by human
- Evaluation formally

- Definition of a decision-making criterion
- Functions to check controls

Process with controls
Risks
Decision-making Criterion

Controls ↔ Risk and control matrices ↔ Risks
Decision-making Criterion

- Control Patterns
- Risk Patterns
- Controls
- Risks
- Risk and control matrices
Decision-making Criterion

- Control Patterns
- Risk Patterns
- Controls
- Risks
- Risk and control matrices
Decision-making Criterion

- Control Patterns
- Risk Patterns
- Controls
- Risks
- Risk and control matrices

- Risk and control matrices
Example: Acceptance of Order (AO)

• **Client**
  – Creating an order form

• **Employees in sales department**
  – Creating an order report from the order form
  – Checking the order report comparing with ledgers
  – Reviewing and Approving the order report
  – Creating and sending confirmation to the client

• **Employees in sales administration department**
  – Booking an order
  – Checking the roster
  – Storing the order form and the order report
Example: Risks

- AO-R1: Accepting fictitious orders.
- AO-R2: Loosing order forms.
- AO-R3: Accepting orders with wrong unit-price.
- AO-R4: Accepting orders without consideration of limit of credit.
- AO-R5: Delivery is overdue.
- AO-R6: Filling in documents for acceptance of order is mistaken.
- AO-R7: Renewing the roster for acceptance of order is mistaken.
- AO-R8: The roster for acceptance of order is cooked.
Example: Controls

- AO-C1: The reception for order reports is specified (e.g. by specified telephone number or fax number).
- AO-C2: Send the confirmation to the client and let him/her check the order.
- AO-C3: Each order report has an ordered ID.
- AO-C4: Rosters are locked to employees in sales department.
- AO-C5: The manager reviews and approves order forms.
- AO-C6: When the price of the product is changed or there is not enough credit, application and approval procedure will be needed.
- AO-C7: The roster is checked by the employee who is not representative after the order is booked.
Example:
Assignments of Controls to Risk

<table>
<thead>
<tr>
<th>AO-R1</th>
<th>AO-C1, AO-C2, AO-C3, AO-C4, AO-C5, AO-C7</th>
</tr>
</thead>
<tbody>
<tr>
<td>AO-R2</td>
<td>AO-C1</td>
</tr>
<tr>
<td>AO-R3</td>
<td>AO-C2, AO-C4, AO-C5, AO-C6</td>
</tr>
<tr>
<td>AO-R4</td>
<td>AO-C4, AO-C5, AO-C6</td>
</tr>
<tr>
<td>AO-R5</td>
<td>AO-C2, AO-C4, AO-C5</td>
</tr>
<tr>
<td>AO-R6</td>
<td>AO-C2, AO-C5</td>
</tr>
<tr>
<td>AO-R7</td>
<td>AO-C7</td>
</tr>
<tr>
<td>AO-R8</td>
<td>AO-C4, AO-C7</td>
</tr>
</tbody>
</table>
Example: Risk Patterns

- **Accepting fictitious transaction**
  - AO-R1 Accepting fictitious orders.

- **Loosing documents**
  - AO-R2 Loosing order forms.

- **A piece of data in a document is wrong**
  - AO-R3 Accepting orders with wrong unit-price.
  - AO-R4 Accepting orders without consideration of limit of credit.
  - AO-R5 Delivery is overdue.

- **Filling in documents is mistaken**
  - AO-R6 Filling in documents for acceptance of order is mistaken.

- **Renewing roster is mistaken**
  - AO-R7 Renewing the roster for acceptance of order is mistaken.

- **Roster is falsified**
  - AO-R8 The roster for acceptance of order is falsified.
Example: Control Patterns

• **Unification of reception**
  – AO-C1: The reception for order reports is specified (e.g. by specified telephone number or fax number).

• **Feedback**
  – AO-C2: Send the confirmation to the client and let him/her check the order.

• **Management of documents with ordered ID**
  – AO-C3: Each order report has an ordered ID.

• **Management of accessibility**
  – AO-C4: Rosters are locked to employees in sales department.

• **Approval by manager**
  – AO-C5: The manager reviews and approves order forms.

• **Exception handling**
  – AO-C6: When the price of the product is changed or there is not enough credit, application and approval procedure will be needed.

• **Operation by non-representative**
  – AO-C7: The roster is checked by the employee who is not representative after the order is booked.
Example: Assignment Pattern

- **Accepting fictitious transaction**:  
  - Unification of reception
  - Management of accessibility
  - Approval by manager
- **Loosing documents**:  
  - Unification of reception
- **A piece of data in a document is wrong**:  
  - Management of accessibility
  - Approval by manager
- **Filling in documents is mistaken**:  
  - Approval by manager
- **Renewing roster is mistaken**:  
  - Approval by manager
- **Roster is falsified**:  
  - Management of accessibility
Behaviour of the Tool

- Accepting fictitious transaction
- Loosing documents
- A piece of data in a document is wrong
- Filling in documents is mistaken
- Renewing roster is mistaken
- Roster is falsified

Risk patterns

Process with controls
Behaviour of the Tool

AO-R1: \( \text{getPlce}(\text{obsDoc}(S, O)) = \text{storage} \) and not(\( \text{obsCWant}(S, CL, O) = \text{getCont}(\text{obsDoc}(S, O)) \))

AO-R2: not(in?(D:Did, \( \text{obsHistory}(S) \)) implies in?(top(\( \text{obsHistory}(S) \))))

AO-R3: \( \text{getPlace}(\text{obsDoc}(S, OR)) = \text{storage} \) and not(\( \text{OK}?(\text{getPid}(\text{obsDoc}(S, OR)), \text{getUPrice}(\text{obsDoc}(S, OR)), \text{getCLid}(\text{obsDoc}(S, OR)))) \))

AO-R4: \( \text{getPlce}(\text{obsDoc}(S, OR)) = \text{storage} \) and not(\( \text{OK}?(\text{getPrice}(\text{obsDoc}(S, OR)), \text{getCLid}(\text{obsDoc}(S, OR)), \text{arledger}) \))

---

Risks

- Accepting fictitious transaction
- Loosing documents
- A piece of data in a document is wrong
- Filling in documents is mistaken
- Renewing roster is mistaken
- Roster is falsified

Risk patterns

- Unification of reception
- Feedback
- Management of documents with ordered ID
- Management of accessibility
- Approval by manager
- Exception handling
- Operation by non-representative

Assignment patterns

- Accepting fictitious transaction
  - Unification of reception
  - Approval by manager
- Loosing documents
  - Unification of reception
  - Management of accessibility
  - Approval by manager
- A piece of data in a document is wrong
  - Management of accessibility
  - Approval by manager
- Filling in documents is mistaken
  - Approval by manager
- Renewing roster is mistaken
  - Approval by manager
- Roster is falsified
  - Management of accessibility

Process with controls

Control patterns
Behaviour of the Tool

Risks

- Accepting fictitious transaction
- Losing documents
- A piece of data in a document is wrong
- Filling in documents is mistaken
- Renewing roster is mistaken
- Roster is falsified

Risk patterns

- Unification of reception
- Management of accessibility
- Approval by manager
- Exception handling
- Operation by non-representative

Assignment patterns

- Accepting fictitious transaction: Unification of reception
- Management of accessibility
- Approval by manager
- Losing documents: Unification of reception
- Management of accessibility
- Approval by manager
- A piece of data in a document is wrong: Unification of reception
- Management of accessibility
- Approval by manager
- Filling in documents is mistaken: Approval by manager
- Renewing roster is mistaken: Approval by manager
- Roster is falsified: Management of accessibility

Process with controls

Control patterns

Department {
  StationName { sales }
  Employee { (E 1) (E 2) }
  Extra { reception }
  Condition { manager(E 2, E 1) ordered(order form)}
  (E 1) { …. }
  (E 2) { …. }
}

Department {
  StationName { sales admin }
  Employee { (E 3) (E 4) }
  (E 3) { …. }
  (E 4) { …. }
}

Client { …. }

21
Control Patterns and Risk Patterns

• In the book*, there are
  – 38 business processes,
  – 174 risks,
  – 221 controls.

• From information in *,
  – 18 control patterns
  – 18 risk patterns

* : M.Sasano, Naibutousei no nyuumon to jissen (Introduction and Practice of Internal Control), 2nd edition, Chuuou Keizaisha, 2007
Conclusion

• Control patterns, risk patterns, and assignment patterns

• Syntactic analysis
  – Checking assignments of controls in descriptions of business processes based on assignment patterns
Analysis of Behaviours

• Modeling the domain as a state transition machine
  – Description of all possible behaviours of the domain
  – States which latent risks exit
  – Formal verification