Business Process Assessment

The selection and implementation of an eSignature system is primarily a business decision rather than a technical one. This section will discuss some of the considerations of both business requirements, as well as risk assessment that should be taken into account prior to deciding on an eSignature system. The business analysis and risk assessment should be considered jointly, not in isolation of each other.

Business Analysis

As noted above, the business process should be the primary determining factor in the selection of an eSignature system. Understanding the business process will drive both the risk analysis as well as the selection of an eSignature solution or solutions. In conducting a business analysis, the following steps should be followed:

- Perform a review of the business process, considering:
    - The transaction's purpose and origins.
    - Its place within the larger business process
    - What services will be delivered and their value to the governmental entity.
    - The various parties to the transaction, including stakeholders who are not directly involved in the transaction, and their business relationships to each other.
    - The transaction's workflow
- Analyze of legal and regulatory requirements, including:
    - How the transaction must be conducted, including timeframes.
    - Signature requirements (e.g., are they specifically required, what records need to be signed, who must or can sign, do they need to be notarized, etc.).
    - Any records-related requirements including:
        - What records must be produced.
        - How long do they need to be retained.
        - Who must or can have access to the records.
        - Specific formats prescribed for the creation, filing or retention of the records.
        - Confidentiality requirements.
    - The degree of importance that the identity of parties to the transaction has to conducting the transaction.
- Identify industry standards or generally accepted practices related to the transaction.
- Analyze those who will use electronically signed records and related requirements.
- Determine interoperability requirements, including those of business partners.
- Determine the cost of alternative approaches.

Risk Assessment

Once you understand the business process you must consider the associated risks. Basically, risk is the *likelihood* that a process or system will be breached in comparison with the degree of *impact* or loss that will be suffered due to said breach. This is usually illustrated as the following matrix:

Risk Assessment Matrix		Impact		
		Low	Medium	High
Likelihood	Low	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	High

Threats

In performing a risk assessment you must identify possible threats and vulnerabilities. Important items to consider include:

- Repudiation – the signer denying having signed the document or denying their intent in signing the document or claiming the document was altered at some time after they signed it
- Fraud – the signer misrepresenting information or forging the signature of another party
- Intrusion – an unauthorized third party gaining access to information in the transaction and exploiting it for personal gain or making other unauthorized use of it
- Loss of records or documentation – electronic documents being lost because they were not preserved or the systems they reside on are unavailable.

Once you have identified the potential threats, you must assess how likely an occurrence each threat is and then further assess the overall likelihood that any threat will occur. Some considerations in determining likelihood include:

- Motivation and capability of the source of the threat.
- Nature of the vulnerability.
- Existence and effectiveness of current controls.

Impact

The impact is the consequence or possible loss of a breach of the system. Some possible impacts include:

- Financial – monetary loss either to the agency, business partners, or the citizen.
- Reputation – public exposure damaging the agency's reputation or the trust the citizens have in the agency. There may also be political repercussions.

Productivity – inability of agency employees or business partners to complete their work in a timely manner, if at all. Additional and otherwise productive time may be spent in addressing the breach and its impact.