Itemized Pricing Sheet

DIR-CPO-4882

Deloitte & Touche LLP

Price Sheet for Services

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Authentication and Authorization - Workforce Identity Management & Governance (Simple, 0 - 999 Customer FTEs)	**Service description:** Deloitte designs and implements user lifecycle management processes utilizing Deloitte's Digital Identity, including user ID naming, integrating with the HR system for identity lifecycle events, and integrating with Active Directory (AD) for user accounts management and access provisioning. Post-implementation, we will work with the customer team to develop a prioritized application integration list, including both on-premises and SaaS applications. Deloitte defines and implements periodic user access review and remediation processes for identified business applications. This includes definition of policy to trigger the user access review process based on user changes in the HR system. **Service activities:** 1. SailPoint IdentityIQ integration for Dev, Test and Production Environments 2. Configure OOTB connectors (such as AD, LDAP, supported applications) in SailPoint IdentityIQ 3. Configure SailPoint CSV connector for applications as an Authoritative feed for internal user lifecycle updates 4. Configure workflows, Provisioning policies for Standard JML /Rehire scenarios(rehire within 60 days of termination, else new user creation) 5. Configure up to two levels of approvals for access requests and standard manager certification 6. Enable Password Management for Active Directory, Configure Reverse Password Sync and Password Expire Notifications 7. Configure AD Group Management functions to update new groups, policy and membership changes 8. Single Sign On (SSO) Integration with SSO solution (if applicable) 9. Configure 5 OOTB SailPoint reports **Service duration:** This service assumes duration of 3 years from start of service. This period includes transition, implementation, configuration and maintenance period. **Assumptions:** 1. Service pricing assumes developmental and configuration effort and Sailpoint IIQ for software licensing. This is included in the Total Price Per User. It does not assume any hosting cost as part of Total Price Per User 2. Workforce Identity Management & Governance assumes a base of 3 Workflows (Joiner, Mover, Leaver) and 5 applications/connectors. 3. Solution hosting and infrastructure is responsibility of customer agency. We will work with customer agency to architect non-production and production environments and submit hardware requirements to customer provider. Deloitte developers are required to get the appropriate access to implement platform and configurations. Deloitte can work with DIR and customer agency to consider hosting costs if customer choses to host this in Deloitte supported cloud hosted environments 4. Project management support will be provided by customer agency to facilitate timely decision-making, change approvals and Product issue resolution 5. Application teams will provide necessary information for dependencies (e.g., services, target host) for specific accounts in order to actively manage the lifecycle within 6. Modifications to OOTB connector or other components are considered customizations. Such customizations are considered out of scope and may require a change order	$ 492.00	Per Customer FTE / yr.	10.00%	$446.12

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Authentication and Authorization - Workforce Identity Management & Governance (Medium, 1000 - 3000 Customer FTEs)	**Service description:** Deloitte designs and implements user lifecycle management processes utilizing Deloitte's Digital Identity, including user ID naming, integrating with the HR system for identity lifecycle events, and integrating with Active Directory (AD) for user accounts management and access provisioning. Post-implementation, we will work with the customer team to develop a prioritized application integration list, including both on-premises and SaaS applications. Deloitte defines and implements periodic user access review and remediation processes for identified business applications. This includes definition of policy to trigger the user access review process based on user changes in the HR system. **Service activities:** 1. SailPoint IdentityIQ integration for Dev, Test and Production Environments 2. Configure OOTB connectors (such as AD, LDAP, supported applications) in SailPoint IdentityIQ 3. Configure SailPoint CSV connector for applications as an Authoritative feed for internal user lifecycle updates 4. Configure workflows, Provisioning policies for Standard JML /Rehire scenarios(rehire within 60 days of termination, else new user creation) 5. Configure up to two levels of approvals for access requests and standard manager certification 6. Enable Password Management for Active Directory, Configure Reverse Password Sync and Password Expire Notifications 7. Configure AD Group Management functions to update new groups, policy and membership changes 8. Single Sign On (SSO) Integration with SSO solution (if applicable) 9. Configure 5 OOTB SailPoint reports **Service duration:** This service assumes duration of 3 years from start of service. This period includes transition, implementation, configuration and maintenance period. **Assumptions:** 1. Service pricing assumes developmental and configuration effort and Sailpoint IIQ for software licensing. This is included in the Total Price Per User. It does not assume any hosting cost as part of Total Price Per User 2. Workforce Identity Management & Governance assumes a base of 3 Workflows (Joiner, Mover, Leaver) and 3 applications/connectors. 3. Solution hosting and infrastructure is responsibility of customer agency. We will work with customer agency to architect non-production and production environments and submit hardware requirements to customer provider. Deloitte developers are required to get the appropriate access to implement platform and configurations. Deloitte can work with DIR and customer agency to consider hosting costs if customer choses to host this in Deloitte supported cloud hosted environments 4. Project management support will be provided by customer agency to facilitate timely decision-making, change approvals and Product issue resolution 5. Application teams will provide necessary information for dependencies (e.g., services, target host) for specific accounts in order to actively manage the lifecycle within 6. Modifications to OOTB connector or other components are considered customizations. Such customizations are considered out of scope and may require a change order	$ 271.00	Per Customer FTE / yr.	10.00%	$245.73

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Authentication and Authorization - Workforce Identity Management & Governance (Large, 3001 - 10000 Customer FTEs)	**Service description:** Deloitte designs and implements user lifecycle management processes utilizing Deloitte's Digital Identity, including user ID naming, integrating with the HR system for identity lifecycle events, and integrating with Active Directory (AD) for user accounts management and access provisioning. Post-implementation, we will work with the customer team to develop a prioritized application integration list, including both on-premises and SaaS applications. Deloitte defines and implements periodic user access review and remediation processes for identified business applications. This includes definition of policy to trigger the user access review process based on user changes in the HR system. **Service activities:** 1. SailPoint IdentityIQ integration for Dev, Test and Production Environments 2. Configure OOTB connectors (such as AD, LDAP, supported applications) in SailPoint IdentityIQ 3. Configure SailPoint CSV connector for applications as an Authoritative feed for internal user lifecycle updates 4. Configure workflows, Provisioning policies for Standard JML /Rehire scenarios(rehire within 60 days of termination, else new user creation) 5. Configure up to two levels of approvals for access requests and standard manager certification 6. Enable Password Management for Active Directory, Configure Reverse Password Sync and Password Expire Notifications 7. Configure AD Group Management functions to update new groups, policy and membership changes 8. Single Sign On (SSO) Integration with SSO solution (if applicable) 9. Configure 5 OOTB SailPoint reports **Service duration:** This service assumes duration of 3 years from start of service. This period includes transition, implementation, configuration and maintenance period. **Assumptions:** 1. Service pricing assumes developmental and configuration effort and Sailpoint IIQ for software licensing. This is included in the Total Price Per User. It does not assume any hosting cost as part of Total Price Per User 2. Workforce Identity Management & Governance assumes a base of 3 Workflows (Joiner, Mover, Leaver) and 3 applications/connectors. 3. Solution hosting and infrastructure is responsibility of customer agency. We will work with customer agency to architect non-production and production environments and submit hardware requirements to customer provider. Deloitte developers are required to get the appropriate access to implement platform and configurations. Deloitte can work with DIR and customer agency to consider hosting costs if customer choses to host this in Deloitte supported cloud hosted environments 4. Project management support will be provided by customer agency to facilitate timely decision-making, change approvals and Product issue resolution 5. Application teams will provide necessary information for dependencies (e.g., services, target host) for specific accounts in order to actively manage the lifecycle within 6. Modifications to OOTB connector or other components are considered customizations. Such customizations are considered out of scope and may require a change order	$ 109.00	Per Customer FTE / yr.	10.00%	$98.84

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Authentication and Authorization - Workforce Identity Management & Governance (Very Large, 10000 - 50000 Customer FTEs)	**Service description:** Deloitte designs and implements user lifecycle management processes utilizing Deloitte's Digital Identity, including user ID naming, integrating with the HR system for identity lifecycle events, and integrating with Active Directory (AD) for user accounts management and access provisioning. Post-implementation, we will work with the customer team to develop a prioritized application integration list, including both on-premises and SaaS applications. Deloitte defines and implements periodic user access review and remediation processes for identified business applications. This includes definition of policy to trigger the user access review process based on user changes in the HR system. **Service activities:** 1. SailPoint IdentityIQ integration for Dev, Test and Production Environments 2. Configure OOTB connectors (such as AD, LDAP, supported applications) in SailPoint IdentityIQ 3. Configure SailPoint CSV connector for applications as an Authoritative feed for internal user lifecycle updates 4. Configure workflows, Provisioning policies for Standard JML /Rehire scenarios(rehire within 60 days of termination, else new user creation) 5. Configure up to two levels of approvals for access requests and standard manager certification 6. Enable Password Management for Active Directory, Configure Reverse Password Sync and Password Expire Notifications 7. Configure AD Group Management functions to update new groups, policy and membership changes 8. Single Sign On (SSO) Integration with SSO solution (if applicable) 9. Configure 5 OOTB SailPoint reports **Service duration:** This service assumes duration of 3 years from start of service. This period includes transition, implementation, configuration and maintenance period. **Assumptions:** 1. Service pricing assumes developmental and configuration effort and Sailpoint IIQ for software licensing. This is included in the Total Price Per User. It does not assume any hosting cost as part of Total Price Per User 2. Workforce Identity Management & Governance assumes a base of 3 Workflows (Joiner, Mover, Leaver) and 3 applications/connectors. 3. Solution hosting and infrastructure is responsibility of customer agency. We will work with customer agency to architect non-production and production environments and submit hardware requirements to customer provider. Deloitte developers are required to get the appropriate access to implement platform and configurations. Deloitte can work with DIR and customer agency to consider hosting costs if customer choses to host this in Deloitte supported cloud hosted environments 4. Project management support will be provided by customer agency to facilitate timely decision-making, change approvals and Product issue resolution 5. Application teams will provide necessary information for dependencies (e.g., services, target host) for specific accounts in order to actively manage the lifecycle within 6. Modifications to OOTB connector or other components are considered customizations. Such customizations are considered out of scope and may require a change order	$ 41.00	Per Customer FTE / yr.	10.00%	$37.18

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Authentication and Authorization - Workforce Access Management (Simple, 0 - 999 Customer FTEs)	**Service description:** Deloitte establishes strong authentication solution, including MFA, to provide an additional layer of protection for prioritized applications. This includes access across applications thereby improving user experience. Our solution integrates with multitude of applications (SaaS, hosted, custom, legacy) via standard-based integrations, gateway or custom patterns. Deloitte will consider risk analysis of the application and client's prioritization to prepare implementation and go-live roadmap for in-scope applications. **Service activities:** 1. Monitor data and user synchronization between on-premise user directory and Okta 2. Monitor directory replication and tune performance 3. Emergency user access disable across all applications 4. Handle requests for delegated admin's in Okta 5. Requests to manage group memberships and access control lists 6. Handle requests to manage attributes in Okta 7. Requests for new trust relationships and Federated SSO setup 8. Verify on-prem directory mastered users as authoritative source synching to Okta 9. SSO to target applications, desktop-SSO or unlock accounts 10. End user access request failures 11. Troubleshoot sign on issues using Okta logs and other monitoring tools **Service duration:** This service assumes duration of 3 years from start of service. This period includes transition, implementation, configuration and maintenance period. **Assumptions:** 1. Service pricing assumes developmental and configuration effort and Okta SaaS for software licensing. This is included in the Total Price Per User. No hosting is assumed as Okta is purely SaaS solution 2. Workforce Access Management assumes a base of base of 10 SSO Applications using standard based integrations (SAML, OAuth, etc.) 3. Standard industry recognized MFA options are utilized such as OTP over SMS, Email and authenticator application 4. Project management support will be provided by customer agency to facilitate timely decision-making, change approvals and Product issue resolution 5. Application teams will provide necessary information for dependencies (e.g., services, target host) for specific accounts in order to actively manage the lifecycle within 6. Modifications to OOTB integrations or other components are considered customizations. Such customizations are considered out of scope and may require a change order	$ 153.00	Per Customer FTE / yr.	10.00%	$138.73

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Authentication and Authorization - Workforce Access Management (Medium, 1000 - 3000 Customer FTEs)	**Service description:** Deloitte establishes strong authentication solution, including MFA, to provide an additional layer of protection for prioritized applications. This includes access across applications thereby improving user experience. Our solution integrates with multitude of applications (SaaS, hosted, custom, legacy) via standard-based integrations, gateway or custom patterns. Deloitte will consider risk analysis of the application and client's prioritization to prepare implementation and go-live roadmap for in-scope applications. **Service activities:** 1. Monitor data and user synchronization between on-premise user directory and Okta 2. Monitor directory replication and tune performance 3. Emergency user access disable across all applications 4. Handle requests for delegated admin's in Okta 5. Requests to manage group memberships and access control lists 6. Handle requests to manage attributes in Okta 7. Requests for new trust relationships and Federated SSO setup 8. Verify on-prem directory mastered users as authoritative source synching to Okta 9. SSO to target applications, desktop-SSO or unlock accounts 10. End user access request failures 11. Troubleshoot sign on issues using Okta logs and other monitoring tools **Service duration:** This service assumes duration of 3 years from start of service. This period includes transition, implementation, configuration and maintenance period. **Assumptions:** 1. Service pricing assumes developmental and configuration effort and Okta SaaS for software licensing. This is included in the Total Price Per User. No hosting is assumed as Okta is purely SaaS solution 2. Workforce Access Management assumes a base of base of 10 SSO Applications using standard based integrations (SAML, OAuth, etc.) 3. Standard industry recognized MFA options are utilized such as OTP over SMS, Email and authenticator application 4. Project management support will be provided by customer agency to facilitate timely decision-making, change approvals and Product issue resolution 5. Application teams will provide necessary information for dependencies (e.g., services, target host) for specific accounts in order to actively manage the lifecycle within 6. Modifications to OOTB integrations or other components are considered customizations. Such customizations are considered out of scope and may require a change order	$ 131.00	Per Customer FTE / yr.	10.00%	$118.78

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Authentication and Authorization - Workforce Access Management (Large, 3000 - 10000 Customer FTEs)	**Service description:** Deloitte establishes strong authentication solution, including MFA, to provide an additional layer of protection for prioritized applications. This includes access across applications thereby improving user experience. Our solution integrates with multitude of applications (SaaS, hosted, custom, legacy) via standard-based integrations, gateway or custom patterns. Deloitte will consider risk analysis of the application and client's prioritization to prepare implementation and go-live roadmap for in-scope applications. **Service activities:** 1. Monitor data and user synchronization between on-premise user directory and Okta 2. Monitor directory replication and tune performance 3. Emergency user access disable across all applications 4. Handle requests for delegated admin's in Okta 5. Requests to manage group memberships and access control lists 6. Handle requests to manage attributes in Okta 7. Requests for new trust relationships and Federated SSO setup 8. Verify on-prem directory mastered users as authoritative source synching to Okta 9. SSO to target applications, desktop-SSO or unlock accounts 10. End user access request failures 11. Troubleshoot sign on issues using Okta logs and other monitoring tools **Service duration:** This service assumes duration of 3 years from start of service. This period includes transition, implementation, configuration and maintenance period. **Assumptions:** 1. Service pricing assumes developmental and configuration effort and Okta SaaS for software licensing. This is included in the Total Price Per User. No hosting is assumed as Okta is purely SaaS solution 2. Workforce Access Management assumes a base of base of 10 SSO Applications using standard based integrations (SAML, OAuth, etc.) 3. Standard industry recognized MFA options are utilized such as OTP over SMS, Email and authenticator application 4. Project management support will be provided by customer agency to facilitate timely decision-making, change approvals and Product issue resolution 5. Application teams will provide necessary information for dependencies (e.g., services, target host) for specific accounts in order to actively manage the lifecycle within 6. Modifications to OOTB integrations or other components are considered customizations. Such customizations are considered out of scope and may require a change order	$ 113.00	Per Customer FTE / yr.	10.00%	$102.46

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Authentication and Authorization - Workforce Access Management (Very Large, 10000 - 50000 Customer FTEs)	**Service description:** Deloitte establishes strong authentication solution, including MFA, to provide an additional layer of protection for prioritized applications. This includes access across applications thereby improving user experience. Our solution integrates with multitude of applications (SaaS, hosted, custom, legacy) via standard-based integrations, gateway or custom patterns. Deloitte will consider risk analysis of the application and client's prioritization to prepare implementation and go-live roadmap for in-scope applications. **Service activities:** 1. Monitor data and user synchronization between on-premise user directory and Okta 2. Monitor directory replication and tune performance 3. Emergency user access disable across all applications 4. Handle requests for delegated admin's in Okta 5. Requests to manage group memberships and access control lists 6. Handle requests to manage attributes in Okta 7. Requests for new trust relationships and Federated SSO setup 8. Verify on-prem directory mastered users as authoritative source synching to Okta 9. SSO to target applications, desktop-SSO or unlock accounts 10. End user access request failures 11. Troubleshoot sign on issues using Okta logs and other monitoring tools **Service duration:** This service assumes duration of 3 years from start of service. This period includes transition, implementation, configuration and maintenance period. **Assumptions:** 1. Service pricing assumes developmental and configuration effort and Okta SaaS for software licensing. This is included in the Total Price Per User. No hosting is assumed as Okta is purely SaaS solution 2. Workforce Access Management assumes a base of base of 10 SSO Applications using standard based integrations (SAML, OAuth, etc.) 3. Standard industry recognized MFA options are utilized such as OTP over SMS, Email and authenticator application 4. Project management support will be provided by customer agency to facilitate timely decision-making, change approvals and Product issue resolution 5. Application teams will provide necessary information for dependencies (e.g., services, target host) for specific accounts in order to actively manage the lifecycle within 6. Modifications to OOTB integrations or other components are considered customizations. Such customizations are considered out of scope and may require a change order	$ 104.00	Per Customer FTE / yr.	10.00%	$94.30

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Authentication and Authorization - Workforce Privileged Access Management (Simple, 0 - 999 Customer FTEs)	**Service description:** Deloitte utilizes its Digital Identity service based on BeyondTrust to onboard and manage privileged accounts for the Windows platform based on customer requirements (Enterprise Administrator accounts, Domain Administrator accounts, Server Local Administrator accounts, Privileged Windows Domain accounts, and Windows Service accounts). This includes implementation of approval processes and audit logging. Automate reporting is included to facilitate audit and compliance. **Service activities:** 1. Proactive monitoring of the state of system infrastructure and components 2. Monitor and detect service availability issues 3. Monitor and verify digital vault VPC availability in cloud deployments 4. Monitor and verify availability of VPN network from cloud to local On prem infrastructure 5. Monitor and verify access to any on-prem vault servers 6. Monitor network connection between VPCs in cloud environment 7. Monitor and verify transit VPC & VPN connections 8. Monitor and verify CPM rotations occur on schedule and check error logs Handle rotation of privileged account credentials which can't be rotated 9. Manage rotation of server vault keys 10. Monitor session recording storage consumption – report and expand per client approval 11. Monitor and verify connectivity from all protected resource subnets 12. Verify administrator self-service password checkout availability 13. Administrative account password resets & issues check-in out credentials 14. Client admin requests for access to privileged account system 15. Admin or device can't initiate connection to protected resource **Service duration:** This service assumes duration of 3 years from start of service. This period includes transition, implementation, configuration and maintenance period **Assumptions:** 1. Service pricing assumes developmental and configuration effort and BeyondTrust PasswordSafe solution for software licensing. This is included in the Total Price Per User. It does not assume any hosting cost as part of Total Price Per User 2. Estimation assumes the number of Privileged Users are 1.67% of the Total Internal Users and there are 10 PAM accounts for each Privileged User. It assumes integration with 3 platform using out of box connectors 3. Solution hosting and infrastructure is responsibility of customer agency. We will work with customer agency to architect non-production and production environments and submit hardware requirements to customer provider. Deloitte developers are required to get the appropriate access to implement platform and configurations. Deloitte can work with DIR and customer agency to consider hosting costs if customer choses to host this in Deloitte supported cloud hosted environments 4. Project management support will be provided by customer agency to facilitate timely decision-making, change approvals and Product issue resolution 5. Application teams will provide necessary information for dependencies (e.g., services, target host) for specific accounts in order to actively manage the lifecycle within 6. Modifications to OOTB platforms or other components are considered customizations. Such customizations are considered out of scope and may require a change order	$ 549.00	Per Customer FTE / yr.	10.00%	$497.81

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Authentication and Authorization - Workforce Privileged Access Management (Medium, 1000 - 3000 Customer FTEs)	**Service description:** Deloitte utilizes its Digital Identity service based on BeyondTrust to onboard and manage privileged accounts for the Windows platform based on customer requirements (Enterprise Administrator accounts, Domain Administrator accounts, Server Local Administrator accounts, Privileged Windows Domain accounts, and Windows Service accounts). This includes implementation of approval processes and audit logging. Automate reporting is included to facilitate audit and compliance. **Service activities:** 1. Proactive monitoring of the state of system infrastructure and components 2. Monitor and detect service availability issues 3. Monitor and verify digital vault VPC availability in cloud deployments 4. Monitor and verify availability of VPN network from cloud to local On prem infrastructure 5. Monitor and verify access to any on-prem vault servers 6. Monitor network connection between VPCs in cloud environment 7. Monitor and verify transit VPC & VPN connections 8. Monitor and verify CPM rotations occur on schedule and check error logs Handle rotation of privileged account credentials which can't be rotated 9. Manage rotation of server vault keys 10. Monitor session recording storage consumption – report and expand per client approval 11. Monitor and verify connectivity from all protected resource subnets 12. Verify administrator self-service password checkout availability 13. Administrative account password resets & issues check-in out credentials 14. Client admin requests for access to privileged account system 15. Admin or device can't initiate connection to protected resource **Service duration:** This service assumes duration of 3 years from start of service. This period includes transition, implementation, configuration and maintenance period **Assumptions:** 1. Service pricing assumes developmental and configuration effort and BeyondTrust PasswordSafe solution for software licensing. This is included in the Total Price Per User. It does not assume any hosting cost as part of Total Price Per User 2. Estimation assumes the number of Privileged Users are 1.67% of the Total Internal Users and there are 10 PAM accounts for each Privileged User. It assumes integration with 3 platform using out of box connectors. 3. Solution hosting and infrastructure is responsibility of customer agency. We will work with customer agency to architect non-production and production environments and submit hardware requirements to customer provider. Deloitte developers are required to get the appropriate access to implement platform and configurations. Deloitte can work with DIR and customer agency to consider hosting costs if customer choses to host this in Deloitte supported cloud hosted environments 4. Project management support will be provided by customer agency to facilitate timely decision-making, change approvals and Product issue resolution 5. Application teams will provide necessary information for dependencies (e.g., services, target host) for specific accounts in order to actively manage the lifecycle within 6. Modifications to OOTB platforms or other components are considered customizations. Such customizations are considered out of scope and may require a change order	$ 310.00	Per Customer FTE / yr.	10.00%	$281.09

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Authentication and Authorization - Workforce Privileged Access Management (Large, 3000 - 10000 Customer FTEs)	**Service description:** Deloitte utilizes its Digital Identity service based on BeyondTrust to onboard and manage privileged accounts for the Windows platform based on customer requirements (Enterprise Administrator accounts, Domain Administrator accounts, Server Local Administrator accounts, Privileged Windows Domain accounts, and Windows Service accounts). This includes implementation of approval processes and audit logging. Automate reporting is included to facilitate audit and compliance. **Service activities:** 1. Proactive monitoring of the state of system infrastructure and components 2. Monitor and detect service availability issues 3. Monitor and verify digital vault VPC availability in cloud deployments 4. Monitor and verify availability of VPN network from cloud to local On prem infrastructure 5. Monitor and verify access to any on-prem vault servers 6. Monitor network connection between VPCs in cloud environment 7. Monitor and verify transit VPC & VPN connections 8. Monitor and verify CPM rotations occur on schedule and check error logs Handle rotation of privileged account credentials which can't be rotated 9. Manage rotation of server vault keys 10. Monitor session recording storage consumption – report and expand per client approval 11. Monitor and verify connectivity from all protected resource subnets 12. Verify administrator self-service password checkout availability 13. Administrative account password resets & issues check-in out credentials 14. Client admin requests for access to privileged account system 15. Admin or device can't initiate connection to protected resource **Service duration:** This service assumes duration of 3 years from start of service. This period includes transition, implementation, configuration and maintenance period **Assumptions:** 1. Service pricing assumes developmental and configuration effort and BeyondTrust PasswordSafe solution for software licensing. This is included in the Total Price Per User. It does not assume any hosting cost as part of Total Price Per User 2. Estimation assumes the number of Privileged Users are 1.67% of the Total Internal Users and there are 10 PAM accounts for each Privileged User. It assumes integration with 3 platform using out of box connectors. 3. Solution hosting and infrastructure is responsibility of customer agency. We will work with customer agency to architect non-production and production environments and submit hardware requirements to customer provider. Deloitte developers are required to get the appropriate access to implement platform and configurations. Deloitte can work with DIR and customer agency to consider hosting costs if customer choses to host this in Deloitte supported cloud hosted environments 4. Project management support will be provided by customer agency to facilitate timely decision-making, change approvals and Product issue resolution 5. Application teams will provide necessary information for dependencies (e.g., services, target host) for specific accounts in order to actively manage the lifecycle within 6. Modifications to OOTB platforms or other components are considered customizations. Such customizations are considered out of scope and may require a change order	$ 131.00	Per Customer FTE / yr.	10.00%	$118.78

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Authentication and Authorization - Workforce Privileged Access Management (Very Large, 10000 - 50000 Customer FTEs)	**Service description:** Deloitte utilizes its Digital Identity service based on BeyondTrust to onboard and manage privileged accounts for the Windows platform based on customer requirements (Enterprise Administrator accounts, Domain Administrator accounts, Server Local Administrator accounts, Privileged Windows Domain accounts, and Windows Service accounts). This includes implementation of approval processes and audit logging. Automate reporting is included to facilitate audit and compliance. **Service activities:** 1. Proactive monitoring of the state of system infrastructure and components 2. Monitor and detect service availability issues 3. Monitor and verify digital vault VPC availability in cloud deployments 4. Monitor and verify availability of VPN network from cloud to local On prem infrastructure 5. Monitor and verify access to any on-prem vault servers 6. Monitor network connection between VPCs in cloud environment 7. Monitor and verify transit VPC & VPN connections 8. Monitor and verify CPM rotations occur on schedule and check error logs Handle rotation of privileged account credentials which can't be rotated 9. Manage rotation of server vault keys 10. Monitor session recording storage consumption – report and expand per client approval 11. Monitor and verify connectivity from all protected resource subnets 12. Verify administrator self-service password checkout availability 13. Administrative account password resets & issues check-in out credentials 14. Client admin requests for access to privileged account system 15. Admin or device can't initiate connection to protected resource **Service duration:** This service assumes duration of 3 years from start of service. This period includes transition, implementation, configuration and maintenance period **Assumptions:** 1. Service pricing assumes developmental and configuration effort and BeyondTrust PasswordSafe solution for software licensing. This is included in the Total Price Per User. It does not assume any hosting cost as part of Total Price Per User 2. Estimation assumes the number of Privileged Users are 1.67% of the Total Internal Users and there are 10 PAM accounts for each Privileged User. It assumes integration with 3 platform using out of box connectors 3. Solution hosting and infrastructure is responsibility of customer agency. We will work with customer agency to architect non-production and production environments and submit hardware requirements to customer provider. Deloitte developers are required to get the appropriate access to implement platform and configurations. Deloitte can work with DIR and customer agency to consider hosting costs if customer choses to host this in Deloitte supported cloud hosted environments 4. Project management support will be provided by customer agency to facilitate timely decision-making, change approvals and Product issue resolution 5. Application teams will provide necessary information for dependencies (e.g., services, target host) for specific accounts in order to actively manage the lifecycle within 6. Modifications to OOTB platforms or other components are considered customizations. Such customizations are considered out of scope and may require a change order	$ 57.00	Per Customer FTE / yr.	10.00%	$51.68

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Endpoint, Network, and Cloud Security - Network boundary protection : Wireless Infrastructure (Large)	**Service description:** The objective of this service is to identify security vulnerabilities in the configuration or implementation of the target wireless LAN infrastructure. As a part of this service, we will perform controlled discovery of wireless access nodes, high level security analysis of the configuration, and assess the overall adequacy of the Wireless LAN infrastructure through the following key tasks: wireless network profile and wireless configuration and security. **Service activities:** 1. Refine scope and plan, identify "trusted agent", gather list in-scope wireless infrastructure access points, agree upon logistics and scanning rules 2. Confirmation of connectivity, tools operation, overview of in-scope application and supporting infrastructure, and gather required credentials and access to perform scanning 3. Perform analysis of the application security controls, including black-box and grey-box testing, perform scans 4. Manual assessment of results, including false-positive and false-negative testing and rationalization of weaknesses noted 5. Confirm observations with trusted agent and stakeholders, and creation of vulnerability assessment report which includes control gaps / weaknesses and corrective action plans **Service duration:** The estimated time for completion is 8 weeks from project start to project end. **Assumptions:** 1. DIR Customer will identify a “trusted agent” responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 2. DIR Customer will provide required credentials to perform testing within three (3) business days of the project start date 3. Deloitte will perform wireless infrastructure review on up to three locations with a total of seventy five (75) wireless access points 4. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within seven (7) business days of submission, and issuance of final deliverable by Deloitte).	$ 198,800.00	Project cost	10.00%	$180,261.90

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Endpoint, Network, and Cloud Security - Network boundary protection : Wireless Infrastructure (Medium)	**Service description:** The objective of this service is to identify security vulnerabilities in the configuration or implementation of the target wireless LAN infrastructure. As a part of this service, we will perform controlled discovery of wireless access nodes, high level security analysis of the configuration, and assess the overall adequacy of the Wireless LAN infrastructure through the following key tasks: wireless network profile and wireless configuration and security. **Service activities:** 1. Refine scope and plan, identify "trusted agent", gather list in-scope wireless infrastructure access points, agree upon logistics and scanning rules 2. Confirmation of connectivity, tools operation, overview of in-scope application and supporting infrastructure, and gather required credentials and access to perform scanning 3. Perform analysis of the application security controls, including black-box and grey-box testing, perform scans 4. Manual assessment of results, including false-positive and false-negative testing and rationalization of weaknesses noted 5. Confirm observations with trusted agent and stakeholders, and creation of vulnerability assessment report which includes control gaps / weaknesses and corrective action plans **Service duration:** The estimated time for completion is 4 weeks from project start to project end. **Assumptions:** 1. DIR Customer will identify a “trusted agent” responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 2. DIR Customer will provide required credentials to perform testing within three (3) business days of the project start date 3. Deloitte will perform wireless infrastructure review on up to three locations with a total of fifty (50) wireless access points 4. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within five (5) business days of submission, and issuance of final deliverable by Deloitte).	$ 99,400.00	Project cost	10.00%	$90,130.95
Endpoint, Network, and Cloud Security - Network boundary protection : Wireless Infrastructure (Simple)	**Service description:** The objective of this service is to identify security vulnerabilities in the configuration or implementation of the target wireless Local Area Network (LAN) infrastructure. As a part of this service, we will perform controlled discovery of wireless access nodes, high level security analysis of the configuration, and assess the overall adequacy of the Wireless LAN infrastructure through the following key tasks: wireless network profile and wireless configuration and security. **Service activities:** 1. Refine scope and plan, identify "trusted agent", gather list in-scope wireless infrastructure access points, agree upon logistics and scanning rules 2. Confirmation of connectivity, tools operation, overview of in-scope application and supporting infrastructure, and gather required credentials and access to perform scanning 3. Perform analysis of the application security controls, including black-box and grey-box testing, perform scans 4. Manual assessment of results, including false-positive and false-negative testing and rationalization of weaknesses noted 5. Confirm observations with trusted agent and stakeholders, and creation of vulnerability assessment report which includes control gaps / weaknesses and corrective action plans **Service duration:** The estimated time for completion is 3 weeks from project start to project end. **Assumptions:** 1. DIR customer will identify a “trusted agent” responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 2. DIR customer will provide required credentials to perform testing within three (3) business days of the project start date	$ 49,700.00	Project cost	10.00%	$45,065.48

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
	3. Deloitte will perform wireless infrastructure review on up to two locations with a total of twenty five (25) wireless access points 4. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within three (3) business days of submission, and issuance of final deliverable by Deloitte).				
Endpoint, Network, and Cloud Security - Remote access security : Remote Access Compromise Analysis (Large)	**Service description:** The purpose of this service is to analyze remote access logs against current cyber intelligence data to expose compromised devices logging into the organization's networks. **Service activities:** Deloitte & Touche LLP ("Deloitte") analyses audit logs up to three (3) Terabytes. **Service duration:** The estimated time for completion is 6 weeks from project start to project end. **Assumptions:** 1. Remote access compromise analysis will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems ("servers, workstations and desktops) within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within three (7) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 148,900.00	Project cost	10.00%	$135,015.08

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Endpoint, Network, and Cloud Security - Remote access security : Remote Access Compromise Analysis (Medium)	**Service description:** The purpose of this service is to analyses remote access logs against current cyber intelligence data to expose compromised devices logging into the organization's networks. **Service activities:** Deloitte & Touche LLP ("Deloitte") analyses audit logs up to two (2) Terabytes. **Service duration:** The estimated time for completion is 4 weeks from project start to project end. **Assumptions:** 1. Remote access compromise analysis will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems ("servers, workstations and desktops) within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within three (5) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 99,200.00	Project cost	10.00%	$89,949.60
Endpoint, Network, and Cloud Security - Remote access security : Remote Access Compromise Analysis (Simple)	**Service description:** The purpose of this service is to analyze remote access logs against current cyber intelligence data to expose compromised devices logging into the organization's networks. **Service activities:** Deloitte & Touche LLP ("Deloitte") analyses audit logs up to one (1) Terabyte. **Service duration:** The estimated time for completion is 3 weeks from project start to project end. **Assumptions:** 1. Remote access compromise analysis will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems ("servers, workstations and desktops) within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within three (7) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 49,600.00	Project cost	10.00%	$44,974.80

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Endpoint, Network, and Cloud Security - Remote access security : Remote Access Compromise Analysis (Very Large)	**Services description:** The purpose of this service is to analyze remote access logs against current cyber intelligence data to expose compromised devices logging into the organization's networks. **Service activities:** Deloitte & Touche LLP ("Deloitte") analyses audit logs up to four (4) Terabytes. **Service duration:** The estimated time for completion is 8 weeks from project start to project end. **Assumptions:** 1. Remote access compromise analysis will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems ("servers, workstations and desktops) within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within three (7) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 198,500.00	Project cost	10.00%	$179,989.88
Endpoint, Network, and Cloud Security - Cloud compliance: Cloud security assessment	**Service description:** This service include performing a Cloud security assessment following the Deloitte & Touche LLP ("Deloitte") methodology, which is based on multiple integrated, industry leading practices and standards. Through a Cloud Cyber Risk Assessment, Deloitte identifies gaps and instances of non-compliance with applicable regulatory requirements, State and Federal laws, as well as local policies. Deloitte leverages an Integrated Risk and Controls Framework as the baseline for the assessment. This Cloud Cyber Risk Framework is a risk-based approach to managing cloud cybersecurity risk. An assessment of a cloud environment includes users, networks, devices, software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to the cloud environment. The principal objective is to reduce the risks, including prevention or mitigation of cybersecurity attacks. The Cloud Cyber Risk Framework provides a common language for understanding, managing, and expressing cloud cybersecurity risk both internally and externally. The Cloud Cyber Risk Framework is used to help identify and prioritize actions for reducing cybersecurity risk in the cloud, and it is a tool for aligning policy, business, and technological approaches to managing that risk. The Cloud Cyber Risk Framework is used to manage cloud cybersecurity risk across entire organizations or it can be focused on the delivery of critical services within an organization. Controls within the Cloud Cyber Risk Framework are sourced through well-known standards and are based on the type of data processed, stored and transmitted by each cloud application or system; the appropriate controls ensure application security by region, industry, and technology. **Service activities:** 1. Conduct the project kick-off, gather relevant information, tailor Deloitte's Framework for a State of Texas agency and socialize the approach with relevant stakeholders. 2. Assess the current posture of a State of Texas agency's cloud usage and associated inherent risk for sanctioned and unsanctioned applications.; 3. Prepare document with inherent risk score, summary and risk details 4. Assess the current posture of specific high priority cloud services in use by the DIR Customer through a combination of top-down and bottom-up approaches as well as scanning of in scope cloud services (as applicable). 5. Define a high level target state for DIR Customer's cloud cyber risk strategic plan by prioritizing relevant risks, and developing recommendations to achieve the target state across people, processes, and tools / technology for each	$ 198,800.00	Project cost	10.00%	$180,261.90

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
	domain. **Service duration:** The estimated time for completion is 8 weeks from project start to project end for assessing one (1) cloud application. **Assumptions:** Cloud Cyber Risk Assessments provide a high-level overview of the current cloud security posture of the assessed agency. The following assumptions were considered during the refinement of DIR Customer pricing: • The assessment will encompass one (1) cloud-based application or environment. • The assessment assumes that DIR Customer stakeholders, subject matter resources, and timely access to the resources who control the various technical systems (inherent risks) and the chosen cloud application (residual risk) in scope. In case DIR Customer's primary personnel are not available during their project duration, the DIR Customer will be responsible for identifying alternative individuals for interviews and support testing • The appropriate stakeholder and business unit representative are available for interviews and workshops for the assessed cloud application or environment are expected the be conducted during the course of the engagement • Weekly status meetings will be attended by project stakeholders; • A part-time project manager will be assigned to assist Deloitte & Touche LLP ("Deloitte") in managing the day-to-day aspects of the project (e.g., scheduling meetings, aligning stakeholders) • DIR Customer will provide the following documents/reports to accelerate initial activities and support the aggressive timeline: o Operational risk framework with risk appetite definitions, o Information security strategy and roadmap, o Information security policies, standards and procedures, o Incident reports and root cause analysis, o Recent audit and regulatory findings, o Information security reports and metrics package, o Third party risk reports, o Tools architecture and current deployment details, o Initiatives / major milestones for security, o Infrastructure architecture diagrams, o Application architecture diagrams, o Run books and maintenance guides for applications, o Proxy/firewall logs will be made available for CASB discovery scan, o System logs will be made available for review, • Access to proxy/firewall logs and the teams that manage these capabilities will be made available to the Deloitte team; • Access to application logs and the teams that manage these capabilities will be made available to the Deloitte team; • Tools used for configuration scans must be given appropriate access to enterprise systems by start of the second week; • DIR Customer is responsible for procurement and licensing of any software beyond what is in scope or considered for use beyond what is included in this document				

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Endpoint, Network, and Cloud Security - Endpoint detection and response (EDR) platforms	**Service description:** The objective of this service is to configure Cylance AI EDR platform on client environment to centrally manage threats to the environment. **Service activities:** 1. Scope and plan, gather list of in-scope systems for installation 2. Determine mechanism in place for deployment 3. Collaborate with System Administrators get package deploy to systems 4. Ensure all scoped systems have agent installed 5. Configure Policies and Playbooks 6. Review Threat Management Dashboard 7. Knowledge Transfer **Service duration:** The estimated time for completion is five (5) weeks depend on the number of assets to be assessed from project start to project end. (time to vary based on the deployment size) **Assumptions:** 1. Assuming that the customer is using Blackberry Cylance. 2. Services provided using Cylance Blackberry Artificial intelligence (AI) driven platform, Cylance Optics. 3. Assuming minimum of 50 Customer FTEs and 200 devices	$ 8.00	Per Customer FTE / yr.	10.00%	$7.25
Endpoint, Network, and Cloud Security - Provide protection of data and services for user devices, network components, applications, and virtual/cloud systems: Security Review - Boundary defense devices	**Service description:** The purpose of this service is to perform a review of the Information Technology (IT) system's security configuration to identify potential vulnerabilities using leading industry practices such as Internal Revenue Service (IRS) Publication 1075 Safeguard Computer Security Evaluation Matrix (SCSEM), National Institute of Standards and Technology (NIST), SANS and Center for Internet Security (CIS). **Service activities:** Perform security configuration review of two boundary defense devices instance such as firewall, intrusion prevention system, antivirus, VPN and switch/router **Service duration:** The estimated time for completion is 3 weeks from project start to project end. **Assumptions:** 1. Security configuration review will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. Security configuration review will require DIR Customer system administrators to provide configuration information from production systems to Deloitte for analysis. 6. DIR Customer will be responsible for remediation of findings 7. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within three (3) business days of submission, and issuance of final deliverable by Deloitte). 8. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 49,600.00	Project cost	10.00%	$44,974.80

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Endpoint, Network, and Cloud Security - Provide protection of data and services for user solution, network components, applications, and virtual/cloud systems: Security Review - Standard ERP Solution	**Service description:** The purpose of this service is to perform a review of the Information Technology (IT) system's security configuration to identify potential vulnerabilities using leading industry practices such as Internal Revenue Service (IRS) Publication 1075 Safeguard Computer Security Evaluation Matrix (SCSEM), National Institute of Standards and Technology (NIST), SANS and Center for Internet Security (CIS). **Service activities:** Perform security configuration review of one standard ERP solution – SAP, PeopleSoft and Oracle Applications **Service duration:** The estimated time for completion is 4 weeks from project start to project end. **Assumptions:** 1. Security configuration review will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. Security configuration review will require DIR Customer system administrators to provide configuration information from production systems to Deloitte for analysis. 6. DIR Customer will be responsible for remediation of findings 7. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within three (3) business days of submission, and issuance of final deliverable by Deloitte). 8. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 99,200.00	Project cost	10.00%	$89,949.60

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Endpoint, Network, and Cloud Security - Provide protection of data and services for user solution, network components, applications, and virtual/cloud systems: Security Review - Standard Operating Systems	**Service description:** The purpose of this service is to perform a review of the Information Technology (IT) system's security configuration to identify potential vulnerabilities using leading industry practices such as Internal Revenue Service Publication (IRS) 1075 Safeguard Computer Security Evaluation Matrix (SCSEM), National Institute of Standards and Technology (NIST), SANS and Center for Internet Security (CIS). **Service activities:** • Perform security configuration review of standard operating system platforms (instance) on up to two (2) information systems: Microsoft Windows (2000, XP, 2003, 2008,7 and 8), UNIX Flavors of HP-UX, AIX, SCO and Tru64, Linux flavors – Red Hat and SuSE, HP OpenVMS, Oracle Solaris • Perform security configuration review of two (2) standard database solution instance – Oracle (SSID), Microsoft SQL Server, MySQL or IBM DB2 • Perform security configuration review of two (2) web server technology instances – Microsoft IIS, Apache Jakarta, Apache Tomcat and IBM WebSphere **Service duration:** The estimated time for completion is 3 weeks from project start to project end. **Assumptions:** 1. Security configuration review will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. Security configuration review will require DIR Customer system administrators to provide configuration information from production systems to Deloitte for analysis. 6. DIR Customer will be responsible for remediation of findings 7. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within three (3) business days of submission, and issuance of final deliverable by Deloitte). 8. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 49,600.00	Project cost	10.00%	$44,974.80

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Endpoint, Network, and Cloud Security - Provide protection of data and services for user solution, network components, applications, and virtual/cloud systems: Security Review - Virtual Infrastructure Instances	**Service description:** The purpose of this service is to perform a review of the Information Technology (IT) system's security configuration to identify potential vulnerabilities using leading industry practices such as Internal Revenue Service Publication (IRS) 1075 Safeguard Computer Security Evaluation Matrix (SCSEM), National Institute of Standards and Technology (NIST), SANS and Center for Internet Security (CIS). **Service activities:** Perform security configuration review of up to three (3) virtual infrastructure instance (VMWare ESX). **Service duration:** The estimated time for completion is 3 weeks from project start to project end. **Assumptions:** 1. Security configuration review will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. Security configuration review will require DIR Customer system administrators to provide configuration information from production systems to Deloitte for analysis. 6. DIR Customer will be responsible for remediation of findings 7. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within three (3) business days of submission, and issuance of final deliverable by Deloitte). 8. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 49,600.00	Project cost	10.00%	$44,974.80

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Endpoint, Network, and Cloud Security - Provide protection of data and services for user system, network components, applications, and virtual/cloud systems: Security Review - Mainframe Operating System	**Service description:** The purpose of this service is to perform a review of the Information Technology (IT) system's security configuration to identify potential vulnerabilities using leading industry practices such as Internal Revenue Service (IRS) Publication 1075 Safeguard Computer Security Evaluation Matrix (SCSEM), National Institute of Standards and Technology (NIST), SANS and Center for Internet Security (CIS). **Service activities:** Perform security configuration review of one mainframe operating system instance – IBM zOS and UNISYS **Service duration:** The estimated time for completion is 4 weeks from project start to project end. **Assumptions:** 1. Security configuration review will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. Security configuration review will require DIR Customer system administrators to provide configuration information from production systems to Deloitte for analysis. 6. DIR Customer will be responsible for remediation of findings 7. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within three (3) business days of submission, and issuance of final deliverable by Deloitte). 8. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 99,200.00	Project cost	10.00%	$89,949.60
Endpoint, Network, and Cloud Security - Network mapping	**Service Description:** The objective of this service is to scan and discover all Network devices in an organization via SNMP and store this information in a database. Then generate Visio compatible Layer 2 and 3 Network topology maps based on the discovery of all devices and interfaces. **Service activities:** 1. Configure SNMP on all devices to be mapped. 2. Deploy and configure Network monitoring appliance. 3. Schedule periodic Network scan to collect all information about devices and interfaces connections. **Service duration:** SNMP configuration and appliance deployment typically takes 3-5 days. Network devices discovery scan will take 2 weeks to ensure all devices are discovered and available for the Network topology map. **Assumptions:** 1. Customer will provide admin level access to all devices to be monitored. 2. Assuming minimum of 50 Customer FTEs and 200 devices	$ 89.00	Per Customer FTE / yr.	10.00%	$80.70

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Endpoint, Network, and Cloud Security - Endpoint protection platforms (EPP)	**Service description:** The objective of this service is to configure Cylance Anti-Virus (Protect) on client systems to effectively manage threats to the environment. **Service activities:** 1. Scope and plan, gather list of in-scope systems for installation 2. Determine mechanism in place for deployment 3. Collaborate with System Administrators get package deploy to systems 4. Ensure all scoped systems have agent installed 5. Configure Policies 6. Review Threat Management Dashboard 7. Knowledge Transfer **Service duration:** The estimated time for completion is five (5) weeks depend on the number of assets to be assessed from project start to project end. (time to vary based on the deployment size) **Assumptions:** 1. Assuming that the customer is using Blackberry Cylance Protect 2. Assuming minimum of 50 Customer FTEs and 200 devices	$ 8.00	Per Customer FTE / yr.	10.00%	$7.25
Endpoint, Network, and Cloud Security - Remote access security	**Service description:** The objective of this service is to provide Two-Factor authentication. DUO integrates with MS clients and Servers to add Two-Factor authentication. **Service activities:** 1. Setup and configure DUO Server on client's Network 2. Link DUO to Active Directory 3. Install and configure client software on desktop and mobile devices. **Service duration:** The estimated time for completion is four (4) weeks from project start to project end. (time to vary based on the deployment size) **Assumptions:** 1. Customer will provide Admin access to all devices to be configured. 2. Assuming that the customer is using DUO product. 3. Assuming minimum of 50 Customer FTEs and 200 devices	$ 6.00	Per Customer FTE / yr.	10.00%	$5.44
Forensic and Incident Response - Network Architecture Documentation	**Service description:** The objective of this service is to document the network infrastructure by passively discovering assets. **Service activities:** 1. Define scope of project 2. Collaborate with key stakeholders on best position of discovery appliance 3. Configure appliance 4. Collect data 5. Analyze Data 6. Review results and determine next step 7. Knowledge transfer **Service duration:** The estimated time for completion is six (6) weeks from project start to project end. (time to vary based on the deployment size) **Assumptions:** 1. Assuming that the customer is using ARMIS platform	$ 20,800.00	Project Cost	10.00%	$18,860.40

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Forensic and Incident Response - Incident Response: Response Preparedness, Incident response plan assessment and enhancement	**Service description:** This service provides DIR Customers with the ability to evaluate their readiness for response preparedness. A cyber incident refers to an adverse event in a company's information systems, and/or network, or the threat of the occurrence of such an event. Deloitte & Touche LLP ("Deloitte") Cyber Incident Response (CIR) methodology is used to assist clients in preparing for and responding to cyber incidents in order to recover their environment impacted by the cyber incident. An iterative approach to CIR provides a repeatable and responsive method to prevent incidents, minimize impact and protect critical data. The incident response lifecycle begins before an incident occurs. A set of proactive and responsive capabilities are required for an organization's operations to rapidly adapt and respond to cyber incidents and continue operations with limited impact to the business. Our broad cyber incident response framework, methodology and services help enable organizations to proactively prepare for a cyber incident and, as needed, the ability to quickly respond to and recover from an incident. **Service activities:** 1. Conduct a gap analysis of the incident response plan against Deloitte's incident response framework. Based on the identified gaps and industry best practices, enhance the incident response plan to close gaps and be broad in nature to represent a holistic response. 2. Conduct a facilitated walkthrough with stakeholders to raise awareness of the new plan. **Service duration:** The estimated time for completion is 8 weeks from project start to project end. **Assumptions:** 1. Scope includes development of incident response (IR) plan only. 2. Scope includes development of three (3) playbooks: To addresses specific cyber-attack vectors (e.g. large scale malware incident, unauthorized access, insider threat/sabotage, data compromise, etc.) as agreed upon with the State. 3. Scope includes one (1) facilitated walkthrough of updated CIR plan with select stakeholders: To review IR plan enhancements. Based on feedback, revise areas of the IR plan and socialize the updated IR plan with select stakeholders. 4. Scope includes development of two (2) quick reference cards: summarizes the IR plan for easier consumption during an incident.	$ 198,800.00	Project cost	10.00%	$180,261.90
Resource, Asset, and Data Protection and Tracking - Asset Discovery	**Service Description:** The objective of this service is to scan and discover all Network devices in an organization and store this information in a database for the purpose of searching and reporting on available assets. **Service activities:** 1. Configure SNMP on all devices 2. Deploy and configure Network scanning appliance 3. Schedule periodic Network scan to monitor device addition or removal. **Service duration:** SNMP configuration and appliance deployment typically takes 3-5 days. Asset discovery scan can take up to 2 weeks to ensure all devices are discovered and recorded in a database. **Assumptions:** 1. Customer will provide admin level access to all devices to be scan/monitored. 2. Assuming minimum of 200 devices	$ 89.00	Per Device / yr.	10.00%	$80.70

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Resource, Asset, and Data Protection and Tracking - Data Leak Protection (DLP)	**Service description:** The objective of this service is to configure Forcepoint DLP in client environment to centrally manage data loss. **Service activities:** 1. Scope and plan, gather list of in-scope systems for installation 2. Determine mechanism in place for deployment 3. Build a Management server 4. Install DLP agents 5. Install Protector 6. Install Web Gateways 7. Configure DLP policies 8. Knowledge transfer **Service duration:** The estimated time for completion is five (5) weeks depend on the number of assets to be assessed from project start to project end. (time to vary based on the deployment size) **Assumptions:** 1. Services provided using customer's Forcepoint DLP platform 2. Assuming minimum of 50 Customer FTEs and 200 devices	$ 24.00	Per Customer FTE / yr.	10.00%	$21.76
Resource, Asset, and Data Protection and Tracking - Encryption	**Service description:** The objective of this service is to install and centrally manage Bitlocker encryption on endpoint. **Service activities:** 1. Scope and plan, gather list of in-scope systems for installation 2. Determine mechanism in place for deployment 3. Determine if license and trusted platform module (TPM) installed support Encryption 4. Configure Management for domain and cloud based computers 5. Configure Bitlocker Recovery, Policies, boot processes 6. Configure central management 7. Knowledge transfer **Service duration:** The estimated time for completion is six (6) weeks depend on the number of assets to be assessed from project start to project end. (time to vary based on the deployment size) **Assumptions:** 1. Desktop/Endpoint encryption using Bitlocker. 2. Assuming minimum of 50 Customer FTEs and 200 devices	$ 8.00	Per Customer FTE / yr.	10.00%	$7.25

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Resource, Asset, and Data Protection and Tracking - Prevent and mitigate loss or breach of classified information: Data Breach Diagnostic (Large)	**Service description:** The purpose of this service is to provide support in identification of the Information Technology (IT) infrastructure impacted by the data breach. Perform a forensic analysis and audit log review of the impacted IT infrastructure to help determine: • How the system(s) were compromised, allowing the data breach to occur • The internal scope of the breach; i.e. How many other systems may have been involved, and may require further investigation/remediation to remove further threat of data loss. • The potential number of Personally Identifiable Information (PII) records affected by the breach **Service activities:** Deloitte & Touche LLP ("Deloitte") performs analysis of fifty (50) systems up to one hundred and twenty (120) Gigabyte (GB) of file storage and up to two (2) Terabyte (TB) of uncompressed text audit logs. **Service duration:** This is estimated as weekly cost to be continued for the duration of project. **Assumptions:** 1. Data breach diagnostic review will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within seven (7) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location. 8. Our personnel will perform all services as a non-testifying consultant. In the event DIR Customer desires to engage Deloitte & Touche LLP ("Deloitte") personnel to testify as an expert witness, both Deloitte and DIR Customer must sign a mutually agreeable, separate, written agreement. 9. We will not provide any legal advice regarding this engagement or any assurance regarding the outcome of any future audit or regulatory examination or other regulatory action. The DIR Customer will be responsible for any legal issues with respect to this engagement, including those arising from the data sources selected and the content of the search results (which may include personally identifiable information or other sensitive third-party information). 10. The DIR Customer understands that based on many factors, including system settings and logging information availability, it may not be possible to identify the source of a compromise or breach or the precise number of records impacted.)	$ 49,600.00	Weekly	10.00%	$44,974.80

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Resource, Asset, and Data Protection and Tracking - Prevent and mitigate loss or breach of classified information: Data Breach Diagnostic (Medium)	**Service description:** The purpose of this service is to provide support in identification of the Information Technology (IT) infrastructure impacted by the data breach. Perform a forensic analysis and audit log review of the impacted IT infrastructure to help determine: • How the system(s) were compromised, allowing the data breach to occur • The internal scope of the breach; i.e. How many other systems may have been involved, and may require further investigation/remediation to remove further threat of data loss. • The potential number of Personally Identifiable Information (PII) records affected by the breach **Service activities:** Deloitte & Touche LLP ("Deloitte") performs analysis of ten (10) systems up to one hundred and twenty (120) Gigabyte (GB) of file storage and up to five hundred (500) GB of uncompressed text audit logs. **Service duration:** This is estimated as weekly cost to be continued for the duration of project. **Assumptions:** 1. Data breach diagnostic review will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within seven (7) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location. 8. Our personnel will perform all services as a non-testifying consultant. In the event DIR Customer desires to engage Deloitte & Touche LLP ("Deloitte") personnel to testify as an expert witness, both Deloitte and DIR Customer must sign a mutually agreeable, separate, written agreement. 9. We will not provide any legal advice regarding this engagement or any assurance regarding the outcome of any future audit or regulatory examination or other regulatory action. The DIR Customer will be responsible for any legal issues with respect to this engagement, including those arising from the data sources selected and the content of the search results (which may include personally identifiable information or other sensitive third-party information). 10. The DIR Customer understands that based on many factors, including system settings and logging information availability, it may not be possible to identify the source of a compromise or breach or the precise number of records impacted.)	$ 24,800.00	Weekly	10.00%	$22,487.40

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Resource, Asset, and Data Protection and Tracking - Prevent and mitigate loss or breach of classified information: Data Breach Diagnostic (Simple)	**Service description:** The purpose of this service is to provide support in identification of the Information Technology infrastructure impacted by the data breach. Perform a forensic analysis and audit log review of the impacted IT infrastructure to help determine: • How the system(s) were compromised, allowing the data breach to occur • The internal scope of the breach; i.e. How many other systems may have been involved, and may require further investigation/remediation to remove further threat of data loss. • The potential number of Personally Identifiable Information (PII) records affected by the breach **Service activities:** Deloitte & Touche LLP ("Deloitte") performs analysis of three (3) systems for up to 120 Gigabyte (GB) of file storage and up to 100 GB of uncompressed text audit logs. **Service duration:** This is estimated as weekly cost to be continued for the duration of project. **Assumptions:** 1. Data breach diagnostic review will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within five (5) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location. 8. Our personnel will perform all services as a non-testifying consultant. In the event DIR Customer desires to engage Deloitte & Touche LLP ("Deloitte") personnel to testify as an expert witness, both Deloitte and DIR Customer must sign a mutually agreeable, separate, written agreement. 9. We will not provide any legal advice regarding this engagement or any assurance regarding the outcome of any future audit or regulatory examination or other regulatory action. The DIR Customer will be responsible for any legal issues with respect to this engagement, including those arising from the data sources selected and the content of the search results (which may include personally identifiable information or other sensitive third-party information). 10. The DIR Customer understands that based on many factors, including system settings and logging information availability, it may not be possible to identify the source of a compromise or breach or the precise number of records impacted.	$ 12,400.00	Weekly	10.00%	$11,243.70

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Resource, Asset, and Data Protection and Tracking - Protect and manage sensitive data	**Service description:** The objective of this service is to configure Forcepoint DLP in client environment to centrally manage data loss. **Service activities:** 1. Scope and plan, gather list of in-scope systems for installation 2. Determine mechanism in place for deployment 3. Build an Management server 4. Install DLP agents 5. Install Protector 6. Install Web Gateways 7. Configure DLP policies 8. Knowledge transfer **Service duration:** The estimated time for completion is five (5) weeks depend on the number of assets to be assessed from project start to project end. (time to vary based on the deployment size) **Assumptions:** 1. Customer is using Forcepoint 2. Assuming minimum of 50 Customer FTEs and 200 devices	$ 24.00	Per Customer FTE / yr.	10.00%	$21.76
Resource, Asset, and Data Protection and Tracking - Sandbox development and testing	**Service description:** As a part of this service, we will configure Cisco AMP and leverage sandboxing through talos and threatgrid **Service activities:** 1. Refine scope and plan, gather list in-scope infrastructure 2. Create planning, test and verification document 3. Configure AMP for endpoints and deploy automated sandbox submissions 4. As-built, reference guide for operations, and knowledge transfer **Service duration:** The estimated time for completion is four (4) weeks from project start to project end. (time to vary based on the deployment size) **Assumptions:** 1. Customer has Cisco AMP for endpoints 2. Assuming minimum of 50 Customer FTEs and 200 devices	$ 24.00	Per Customer FTE / yr.	10.00%	$21.76
Resource, Asset, and Data Protection and Tracking - Virtual Private Networks (VPN)	**Service description:** The objective of this service is to provide VPN services to client Networks using customer's Cisco or Palo Alto hardware. **Service activities:** 1. Configure new or existing Firewall hardware 2. Install and configure VPN client on end point devices **Service duration:** The estimated time for completion is four (4) weeks from project start to project end. (time to vary based on the deployment size) **Assumptions:** 1. Customer will provide Admin access to all devices to be configured 2. Assuming minimum of 200 devices	$ 89.00	Per Device / yr.	10.00%	$80.70

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Threat Detection and Security Monitoring - Anomaly and event detection: Insider Threat Detection Diagnostic (Large)	**Service description:** The purpose of this service is to conduct an assessment of the organization's insider threat detection capability including review of existing logs that can reveal current or past insider threats. The review will also examine recent incidents and recommend a roadmap for automating the capability. **Service activities:** Deloitte & Touche LLP ("Deloitte") performs and assessment of the current state of a mid-sized agency (1,000-9,999 employees), up to one (1) Terabyte (TB) of audit log files and conduct up to ten (10) interviews. **Service duration:** The estimated time for completion is 6 weeks from project start to project end. **Assumptions:** 1. Insider threat detection diagnostic analysis will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems ("servers, workstations and desktops) within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within seven (7) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 148,900.00	Project cost	10.00%	$135,015.08
Threat Detection and Security Monitoring - Anomaly and event detection: Insider Threat Detection Diagnostic (Medium)	**Service description:** The purpose of this service is to conduct an assessment of the organization's insider threat detection capability including review of existing logs that can reveal current or past insider threats. The review will also examine recent incidents and recommend a roadmap for automating the capability. **Service activities:** Deloitte & Touche LLP ("Deloitte") performs an assessment of the current state of a small sized agency (100-999 employees), up to five hundred (500) Gigabyte (GB) of audit log files and conduct up to five (5) interviews. **Service duration:** The estimated time for completion is 4 weeks from project start to project end. **Assumptions:** 1. Insider threat detection diagnostic analysis will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems ("servers, workstations and desktops) within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within five (5) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be	$ 99,200.00	Project cost	10.00%	$89,949.60

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
	available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.				
Threat Detection and Security Monitoring - Anomaly and event detection: Insider Threat Detection Diagnostic (Simple)	**Service description:** The purpose of this service is to conduct an assessment of the organization's insider threat detection capability including review of existing logs that can reveal current or past insider threats. The review will also examine recent incidents and recommend a roadmap for automating the capability. **Service activities** Deloitte & Touche LLP ("Deloitte") performs an assessment of the current state of a very-small sized agency (1-99 employees), up to two hundred and fifty (250) Gigabyte (GB) of audit log files and conduct up to three (3) interviews. **Service duration:** The estimated time for completion is 3 weeks from project start to project end. **Assumptions:** 1. Insider threat detection diagnostic analysis will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems ("servers, workstations and desktops) within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within three (3) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 49,600.00	Project cost	10.00%	$44,974.80

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Threat Detection and Security Monitoring - Anomaly and event detection: Insider Threat Detection Diagnostic (Very Large)	**Service description:** The purpose of this service is to conduct an assessment of the organization's insider threat detection capability including review of existing logs that can reveal current or past insider threats. The review will also examine recent incidents and recommend a roadmap for automating the capability. **Service activities:** Deloitte & Touche LLP ("Deloitte") performs and assessment of the current state of a large sized agency (>10,000 employees), up to two (2) Terabyte (TB) of audit log files and conduct up to three (3) interviews. **Service duration:** The estimated time for completion is 8 weeks from project start to project end. **Assumptions:** 1. Insider threat detection diagnostic analysis will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems ("servers, workstations and desktops) within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within seven (7) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 198,500.00	Project cost	10.00%	$179,989.88
Threat Detection and Security Monitoring - Anomaly and event detection: Suspicious Program Diagnostic (Large)	**Services description:** The purpose of this service is to identify potentially unwanted programs, malicious files, and unknown binaries on agency workstations and desktops. **Service activities:** Deloitte & Touche LLP ("Deloitte") assess up to two hundred and fifty (250) standard configuration of servers, workstations and desktops. **Service duration:** The estimated time for completion is 8 weeks from project start to project end. **Assumptions:** 1. Suspicious program diagnostic will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems ("servers, workstations and desktops) within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within three (7) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 198,500.00	Project cost	10.00%	$179,989.88

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Threat Detection and Security Monitoring - Anomaly and event detection: Suspicious Program Diagnostic (Medium)	**Service description:** The purpose of this service is to identify potentially unwanted programs, malicious files, and unknown binaries on agency workstations and desktops. **Service activities:** Deloitte & Touche LLP ("Deloitte") assess up to one hundred (100) standard configuration of servers, workstations and desktops. **Service duration:** The estimated time for completion is 4 weeks from project start to project end. **Assumptions:** 1. Suspicious program diagnostic will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems ("servers, workstations and desktops) within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within three (5) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 99,200.00	Project cost	10.00%	$89,949.60
Threat Detection and Security Monitoring - Anomaly and event detection: Suspicious Program Diagnostic (Simple)	**Services description:** The purpose of this service is to identify potentially unwanted programs, malicious files, and unknown binaries on agency workstations and desktops. **Service activities:** Deloitte & Touche LLP ("Deloitte") performs assessment on up to twenty five (25) standard configuration of servers, workstations and desktops. **Service duration:** The estimated time for completion is 3 weeks from project start to project end. **Assumptions:** 1. Suspicious program diagnostic will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems ("servers, workstations and desktops) within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within three (3) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 49,600.00	Project cost	10.00%	$44,974.80

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Threat Detection and Security Monitoring - Anomaly and event detection: Suspicious Program Diagnostic (Very Large)	**Services description:** The purpose of this service is to identify potentially unwanted programs, malicious files, and unknown binaries on agency workstations and desktops. **Service activities:** Deloitte & Touche LLP ("Deloitte") assess up to 1,000 standard configuration of servers, workstations and desktops. **Service duration:** The estimated time for completion is 10 weeks from project start to project end. **Assumptions:** 1. Suspicious program diagnostic will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems ("servers, workstations and desktops) within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within three (7) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 248,100.00	Project cost	10.00%	$224,964.68
Threat Detection and Security Monitoring - Provide continuous security monitoring and threat detection - Threat Research (Large)	**Service description:** This services provides DIR customers with an analysis of security event logs to identify those potential internal hosts that may be compromised and are attempting to communicate with malicious internet hosts. The analysis will include detection of potential internal devices to determine if any of them are rogue or exhibiting stealth-like characteristics. **Service activities:** Deloitte & Touche LLP ("Deloitte") analyses audit logs up to three (3) Tera Bytes. Perform rogue device discovery up to 3,500 system. **Service duration:** The estimated time for completion is 6 weeks from project start to project end. **Assumptions:** 1. Threat research will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the audit logs within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within seven (7) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 148,900.00	Project cost	10.00%	$135,015.08

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Threat Detection and Security Monitoring - Provide continuous security monitoring and threat detection - Threat Research (Medium)	**Services description:** This services provides DIR customers with an analysis of security event logs to identify those potential internal hosts that may be compromised and are attempting to communicate with malicious internet hosts. The analysis will include detection of potential internal devices to determine if any of them are rogue or exhibiting stealth-like characteristics. **Service activities:** Deloitte & Touche LLP ("Deloitte") analyses audit logs up to two (2) Tera Byte. Perform rogue device discovery up to 2,000 systems. **Service duration:** The estimated time for completion is 4 weeks from project start to project end. **Assumptions:** 1. Threat research will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the audit logs within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within five (5) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 99,200.00	Project cost	10.00%	$89,949.60
Threat Detection and Security Monitoring - Provide continuous security monitoring and threat detection - Threat Research (Simple)	**Services description:** This service provides DIR customers with an analysis of security event logs to identify those potential internal hosts that may be compromised and are attempting to communicate with malicious internet hosts. The analysis will include detection of potential internal devices to determine if any of them are rogue or exhibiting stealth-like characteristics. **Service activities:** Deloitte & Touche LLP ("Deloitte") analyses audit logs up to two (1) Tera Byte. Perform rogue device discovery up to thousand (1000) systems. **Service duration:** The estimated time for completion is 3 weeks from project start to project end. **Assumptions:** 1. Threat research will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the audit logs within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within three (3) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be	$ 74,400.00	Project cost	10.00%	$67,462.20

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
	available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.				
Threat Detection and Security Monitoring - Provide continuous security monitoring and threat detection - Threat Research (Very Large)	**Services description:** This services provides DIR customers with an analysis of security event logs to identify those potential internal hosts that may be compromised and are attempting to communicate with malicious internet hosts. The analysis will include detection of potential internal devices to determine if any of them are rogue or exhibiting stealth-like characteristics. **Service activities:** Deloitte & Touche LLP ("Deloitte") analyses audit logs up to four (4) Tera Bytes. Perform rogue device discovery up to 5,000 systems. **Service duration:** The estimated time for completion is 8 weeks from project start to project end. **Assumptions:** 1. Threat research will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the audit logs within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within seven (7) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 198,500.00	Project cost	10.00%	$179,989.88

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Threat Detection and Security Monitoring - Provide continuous security monitoring and threat detection: Log Management & Analysis	**Service description:** The objective of this service is to assist DIR customers detect targeted threats and sensitive information disclosures. The service provides DIR customers with 24 X 7 threat monitoring using the correlation capabilities of their security information and event management (SIEM) system to help detect anomalous activity that could be indicative of unauthorized activity. Working with the client, Deloitte & Touche LLP ("Deloitte") also defines SIEM use cases to align with their specific monitoring requirements. Deloitte collaborates with DIR customers to plan critical security monitoring objectives to business risk and compliance requirements; mature implemented monitoring solutions; and measure effectiveness in quarterly cycles. **Service activities:** Deloitte performs Security Monitoring using the DIR customer's existing SIEM to monitor their enterprise information technology environment. The service includes: 1. Provide 24x7x365 event monitoring and security analysis of the enterprise information technology environment via SIEM, including perimeter firewalls, intrusion prevention systems/intrusion detection systems (IPS/IDS) web/email security gateways, and other. 2. Provide real/near real-time alert research, triage and escalation of potential incidents to DIR customers, in-house security staff using a pre-established prioritization matrix. 3. Provide 24 X 7 automated alerting on SIEM status, business hours remediation of identified issues, and annual upgrades to the SIEM. 4. Design and implementation of custom SIEM content items (alert, report, dashboard) to meet customer business requirements. 5. Provide in-depth information security experience in security event identification, correlation and analysis, and log management. 6. Provide ad hoc support of the customer's security incident handling team. Deloitte leverages its Managed Threat Services (MTS) group to execute these tasks and provide value to DIR customers. The MTS model of shared service infrastructure, resources, and knowledge provides compelling benefits to DIR customers, allowing DIR to leverage our years of experience providing similar services to large clients to achieve operational efficiencies and cost-savings. **Service duration:** The estimated time for these services is twelve (12) months from project start to project end. **Assumptions:** 1. Threat monitoring costs are tied to environment size as expressed in events per second; environment size is used as a proxy for the approximate level of effort to staff 24 X 7 monitoring and meet agreed-upon SLAs for service delivery. 24 X 7 monitoring assumes environment size of three thousand (3000) events per second (EPS) and alert volume of approximately fifty (50) alerts per day (after content tuning). 2. Monitoring is based on analyst response to SIEM alerts and is not "eyes on glass." Services are provided from Deloitte Security Operations Centers (SOCs) located in the United States. 3. Deloitte assumes that DIR customer will have an existing SIEM system that is operational and configured to collect logs. DIR customer will provide Deloitte cyber security specialist with remote access to the SIEM. 4. Deloitte proposed service activities are subject to a mutually agreed-upon engagement letter and general business terms and conditions between Deloitte and DIR customer. 5. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 1,389,300.00	Project cost	10.00%	$1,259,747.78

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Threat Detection and Security Monitoring - Vulnerability scanning and management : Application Code Review Scanning (Large)	**Service description:** The objective of this service is to use static code review tools to perform security code review for identification of potential insecure coding practices within the custom web application source code. Supported custom web application technologies: Microsoft .NET framework, JAVA, Adobe Flash, JavaScript and AJAX. We will map the confirmed vulnerabilities to the top ten (10) vulnerability categories of Open Web Application Security Project (OWASP). **Service activities:** 1. Refine scope and plan, identify "trusted agent", gather list in-scope application and supporting infrastructure, agree upon logistics and scanning rules 2. Confirmation of connectivity, tools operation, overview of in-scope application and supporting infrastructure, and gather required credentials and access to perform scanning 3. Perform analysis of the application security controls, including black-box and grey-box testing, perform scans 4. Manual assessment of results, including false-positive and false-negative testing and rationalization of weaknesses noted 5. Confirm observations with trusted agent and stakeholders, and creation of vulnerability assessment report which includes control gaps / weaknesses and corrective action plans **Service duration:** The estimated time for completion is 6 weeks from project start to project end. **Assumptions:** 1. Vulnerability scanning will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. 2. Vulnerability scanning will be performed in a non-production environment that minimizes disruption to business services 3. DIR Customer will identify a “trusted agent” responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 4. DIR Customer will facilitate remote access to the non-production application within three (3) business days of the project start date 5. DIR Customer will provide required credentials to perform testing within three (3) business days of the project start date 6. DIR Customer Price provided is on a per application basis (one application) 7. DIR Customer will be responsible for remediation of findings 8. Deloitte will perform a security code review on up to two (2) million lines of one (1) web application custom source code. Perform manual verification on up to twenty five (25) vulnerabilities (up to eight instances per vulnerability assimilated) 9. Deliverable acceptance process includes one (1) review cycles (1 draft submitted for review, written feedback provided to Deloitte within seven (7) business days of submission, and issuance of final deliverable by Deloitte). 10. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 149,100.00	Project cost	10.00%	$135,196.43

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Threat Detection and Security Monitoring - Vulnerability scanning and management : Application Code Review Scanning (Medium)	**Service description:** The objective of this service is to use static code review tools to perform security code review for identification of potential insecure coding practices within the custom web application source code. Supported custom web application technologies: Microsoft .NET framework, JAVA, Adobe Flash, JavaScript and AJAX. We will map the confirmed vulnerabilities to the top ten (10) vulnerability categories of Open Web Application Security Project (OWASP). **Service activities:** 1. Refine scope and plan, identify "trusted agent", gather list in-scope application and supporting infrastructure, agree upon logistics and scanning rules 2. Confirmation of connectivity, tools operation, overview of in-scope application and supporting infrastructure, and gather required credentials and access to perform scanning 3. Perform analysis of the application security controls, including black-box and grey-box testing, perform scans 4. Manual assessment of results, including false-positive and false-negative testing and rationalization of weaknesses noted 5. Confirm observations with trusted agent and stakeholders, and creation of vulnerability assessment report which includes control gaps / weaknesses and corrective action plans **Service duration:** The estimated time for completion is 4 weeks from project start to project end. **Assumptions:** 1. Vulnerability scanning will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. 2. Vulnerability scanning will be performed in a non-production environment that minimizes disruption to business services 3. DIR Customer will identify a “trusted agent” responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 4. DIR Customer will facilitate remote access to the non-production application within three (3) business days of the project start date 5. DIR Customer will provide required credentials to perform testing within three (3) business days of the project start date 6. DIR Customer Price provided is on a per application basis (one application) 7. DIR Customer will be responsible for remediation of findings 8. Deloitte will perform a security code review on up to one (1) million lines of one (1) web application custom source code. Perform manual verification on up to twenty (20) vulnerabilities (up to six instances per vulnerability assimilated) 9. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within five (5) business days of submission, and issuance of final deliverable by Deloitte) 10. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 99,400.00	Project cost	10.00%	$90,130.95

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Threat Detection and Security Monitoring - Vulnerability scanning and management : Application Code Review Scanning (Simple)	**Service description:** The objective of this service is to use static code review tools to perform security code review for identification of potential insecure coding practices within the custom web application source code. Supported custom web application technologies: Microsoft .NET framework, JAVA, Adobe Flash, JavaScript and AJAX. We will map the confirmed vulnerabilities to the top ten (10) vulnerability categories of Open Web Application Security Project (OWASP). **Service activities:** 1. Refine scope and plan, identify "trusted agent", gather list in-scope application and supporting infrastructure, agree upon logistics and scanning rules 2. Confirmation of connectivity, tools operation, overview of in-scope application and supporting infrastructure, and gather required credentials and access to perform scanning 3. Perform analysis of the application security controls, including black-box and grey-box testing, perform scans 4. Manual assessment of results, including false-positive and false-negative testing and rationalization of weaknesses noted 5. Confirm observations with trusted agent and stakeholders, and creation of vulnerability assessment report which includes control gaps / weaknesses and corrective action plans **Service duration:** The estimated time for completion is 3 weeks from project start to project end. **Assumptions:** 1. Vulnerability scanning will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. 2. Vulnerability scanning will be performed in a non-production environment that minimizes disruption to business services 3. DIR Customer will identify a “trusted agent” responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 4. DIR Customer will facilitate remote access to the non-production application within three (3) business days of the project start date 5. DIR Customer will provide required credentials to perform testing within three (3) business days of the project start date 6. DIR Customer Price provided is on a per application basis (one application) 7. DIR Customer will be responsible for remediation of findings 8. Deloitte will perform a security code review on up to five hundred thousand (500,000) lines of one web application custom source code. Perform manual verification on up to fifteen (15) vulnerabilities (up to four instances per vulnerability assimilated) 9. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within three (3) business days of submission, and issuance of final deliverable by Deloitte) 10. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 49,700.00	Project cost	10.00%	$45,065.48

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Threat Detection and Security Monitoring - Vulnerability scanning and management : Application Code Review Scanning (Very Large)	**Service description:** The objective of this service is to use static code review tools to perform security code review for identification of potential insecure coding practices within the custom web application source code. Supported custom web application technologies: Microsoft .NET framework, JAVA, Adobe Flash, JavaScript and AJAX. We will map the confirmed vulnerabilities to the top ten (10) vulnerability categories of Open Web Application Security Project (OWASP). **Service activities:** 1. Refine scope and plan, identify "trusted agent", gather list in-scope application and supporting infrastructure, agree upon logistics and scanning rules 2. Confirmation of connectivity, tools operation, overview of in-scope application and supporting infrastructure, and gather required credentials and access to perform scanning 3. Perform analysis of the application security controls, including black-box and grey-box testing, perform scans 4. Manual assessment of results, including false-positive and false-negative testing and rationalization of weaknesses noted 5. Confirm observations with trusted agent and stakeholders, and creation of vulnerability assessment report which includes control gaps / weaknesses and corrective action plans **Service duration:** The estimated time for completion is 10 weeks from project start to project end. **Assumptions:** 1. Vulnerability scanning will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. 2. Vulnerability scanning will be performed in a non-production environment that minimizes disruption to business services 3. DIR Customer will identify a “trusted agent” responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 4. DIR Customer will facilitate remote access to the non-production application within three (3) business days of the project start date 5. DIR Customer will provide required credentials to perform testing within three (3) business days of the project start date 6. DIR Customer Price provided is on a per application basis (one application) 7. DIR Customer will be responsible for remediation of findings 8. Deloitte will perform a security code review on up to three (3) million lines of one (1) web application custom source code. Perform manual verification on up to thirty five (35) vulnerabilities (up to 10 instances per vulnerability assimilated) 9. Deliverable acceptance process includes one (1) review cycles (1 draft submitted for review, written feedback provided to Deloitte within seven (7) business days of submission, and issuance of final deliverable by Deloitte). 10. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 248,500.00	Project cost	10.00%	$225,327.38

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Threat Detection and Security Monitoring - Vulnerability scanning and management : Database Scanning (Large)	**Service description:** The objective of this service is to perform a controlled vulnerability assessment on the target database infrastructure to identify potential security vulnerabilities that may lead to unauthorized information leakage or even lead to comprise of the database system. Supported database assessments: Oracle, Microsoft SQL Server, IBM DB2, MySQL, Lotus Domino and Sybase. **Service activities:** 1. Refine scope and plan, identify "trusted agent", gather list in-scope application database and supporting infrastructure, agree upon logistics and scanning rules 2. Confirmation of connectivity, tools operation, overview of in-scope application and supporting infrastructure, and gather required credentials and access to perform scanning 3. Perform analysis of the application security controls, including black-box and grey-box testing, perform scans 4. Manual assessment of results, including false-positive and false-negative testing and rationalization of weaknesses noted 5. Confirm observations with trusted agent and stakeholders, and creation of vulnerability assessment report which includes control gaps / weaknesses and corrective action plans **Service duration:** The estimated time for completion is 6 weeks from project start to project end. **Assumptions:** 1. Vulnerability scanning will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. 2. Vulnerability scanning will be performed in a non-production environment that minimizes disruption to business services 3. DIR customer will identify a “trusted agent” responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 4. DIR customer will facilitate remote access to the non-production application within three (3) business days of the project start date 5. DIR customer will provide required credentials to perform testing within three (3) business days of the project start date 6. DIR Customer Price provided is on a per a DIR Customer Price provided is on a per database basis (one database) 7. DIR Customer will be responsible for remediation of findings 8. Deloitte will perform a vulnerability assessment on up to ten (10) database servers running up to fifteen (15) instances/Oracle SIDs 9. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within seven (7) business days of submission, and issuance of final deliverable by Deloitte). 10. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 149,100.00	Project cost	10.00%	$135,196.43

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Threat Detection and Security Monitoring - Vulnerability scanning and management : Database Scanning (Medium)	**Service description:** The objective of this service is to perform a controlled vulnerability assessment on the target database infrastructure to identify potential security vulnerabilities that may lead to unauthorized information leakage or even lead to comprise of the database system. Supported database assessments: Oracle, Microsoft SQL Server, IBM DB2, MySQL, Lotus Domino and Sybase. **Service activities:** 1. Refine scope and plan, identify "trusted agent", gather list in-scope application database and supporting infrastructure, agree upon logistics and scanning rules 2. Confirmation of connectivity, tools operation, overview of in-scope application and supporting infrastructure, and gather required credentials and access to perform scanning 3. Perform analysis of the application security controls, including black-box and grey-box testing, perform scans 4. Manual assessment of results, including false-positive and false-negative testing and rationalization of weaknesses noted 5. Confirm observations with trusted agent and stakeholders, and creation of vulnerability assessment report which includes control gaps / weaknesses and corrective action plans **Service duration:** The estimated time for completion is 4 weeks from project start to project end. **Assumptions:** 1. Vulnerability scanning will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. 2. Vulnerability scanning will be performed in a non-production environment that minimizes disruption to business services 3. DIR Customer will identify a “trusted agent” responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 4. DIR Customer will facilitate remote access to the non-production application within three (3) business days of the project start date 5. DIR Customer will provide required credentials to perform testing within three (3) business days of the project start date 6. DIR Customer Price provided is on a per database basis (one database) 7. DIR Customer will be responsible for remediation of findings 8. Deloitte will perform a vulnerability assessment on up to five (5) database servers running up to ten (10) instances/Oracle SIDs 9. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within five (5) business days of submission, and issuance of final deliverable by Deloitte). 10. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 99,400.00	Project cost	10.00%	$90,130.95

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Threat Detection and Security Monitoring - Vulnerability scanning and management : Database Scanning (Simple)	**Service description:** The objective of this service is to perform a controlled vulnerability assessment on the target database infrastructure to identify potential security vulnerabilities that may lead to unauthorized information leakage or even lead to comprise of the database system. Supported database assessments: Oracle, Microsoft SQL Server, IBM DB2, MySQL, Lotus Domino and Sybase. **Service activities:** 1. Refine scope and plan, identify "trusted agent", gather list in-scope application database and supporting infrastructure, agree upon logistics and scanning rules 2. Confirmation of connectivity, tools operation, overview of in-scope application and supporting infrastructure, and gather required credentials and access to perform scanning 3. Perform analysis of the application security controls, including black-box and grey-box testing, perform scans 4. Manual assessment of results, including false-positive and false-negative testing and rationalization of weaknesses noted 5. Confirm observations with trusted agent and stakeholders, and creation of vulnerability assessment report which includes control gaps / weaknesses and corrective action plans **Service duration:** The estimated time for completion is 3 weeks from project start to project end. **Assumptions:** 1. Vulnerability scanning will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. 2. Vulnerability scanning will be performed in a non-production environment that minimizes disruption to business services 3. DIR Customer will identify a “trusted agent” responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 4. DIR Customer will facilitate remote access to the non-production application within three (3) business days of the project start date 5. DIR Customer will provide required credentials to perform testing within three (3) business days of the project start date 6. DIR Customer Price provided is on a per database basis (one database) 7. DIR Customer will be responsible for remediation of findings 8. Deloitte will perform a vulnerability assessment on up to three (3) database servers running up to five (5) instances/Oracle SIDs 9. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within three (3) business days of submission, and issuance of final deliverable by Deloitte). 10. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 49,700.00	Project cost	10.00%	$45,065.48

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Threat Detection and Security Monitoring - Vulnerability scanning and management : Database Scanning (Very Large)	**Service description:** The objective of this service is to perform a controlled vulnerability assessment on the target database infrastructure to identify potential security vulnerabilities that may lead to unauthorized information leakage or even lead to comprise of the database system. Supported database assessments: Oracle, Microsoft SQL Server, IBM DB2, MySQL, Lotus Domino and Sybase. **Service activities:** 1. Refine scope and plan, identify "trusted agent", gather list in-scope application database and supporting infrastructure, agree upon logistics and scanning rules 2. Confirmation of connectivity, tools operation, overview of in-scope application and supporting infrastructure, and gather required credentials and access to perform scanning 3. Perform analysis of the application security controls, including black-box and grey-box testing, perform scans 4. Manual assessment of results, including false-positive and false-negative testing and rationalization of weaknesses noted 5. Confirm observations with trusted agent and stakeholders, and creation of vulnerability assessment report which includes control gaps / weaknesses and corrective action plans **Service duration:** The estimated time for completion is 8 weeks from project start to project end. **Assumptions:** 1. Vulnerability scanning will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. 2. Vulnerability scanning will be performed in a non-production environment that minimizes disruption to business services 3. DIR customer will identify a “trusted agent” responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 4. DIR customer will facilitate remote access to the non-production application within three (3) business days of the project start date 5. DIR customer will provide required credentials to perform testing within three (3) business days of the project start date 6. DIR Customer Price provided is on a per a DIR Customer Price provided is on a per database basis (one database) 7. DIR Customer will be responsible for remediation of findings 8. Deloitte will perform a vulnerability assessment on up to twenty (20) database servers running up to thirty (30) instances/Oracle SIDs 9. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within seven (7) business days of submission, and issuance of final deliverable by Deloitte). 10. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 198,800.00	Project cost	10.00%	$180,261.90

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Threat Detection and Security Monitoring - Vulnerability scanning and management : Web Application Scanning (Large)	**Service description:** The objective of this service it to identify potential vulnerabilities which might be used by attackers to compromise web-based applications, the data within the applications, and / or supporting infrastructure. As part of our service offering, we will perform automated vulnerability tests and use manual testing techniques along with our proprietary knowledgebase of application attack profiles and web server vulnerabilities to test the application servers for possible exposures to vulnerabilities. We will map the confirmed vulnerabilities to the top ten (10) vulnerability categories of Open Web Application Security Project (OWASP). **Service activities:** 1. Refine scope and plan, identify "trusted agent", gather list in-scope web applications and supporting infrastructure, agree upon logistics and scanning rules 2. Confirmation of connectivity, tools operation, overview of in-scope applications and supporting infrastructure, and gather required credentials and access to perform scanning 3. Perform analysis of the application security controls, including black-box and grey-box testing, perform scans 4. Manual assessment of results, including false-positive and false-negative testing and rationalization of weaknesses noted 5. Confirm observations with trusted agent and stakeholders, and creation of vulnerability assessment report which includes control gaps / weaknesses and corrective action plans **Service duration:** The estimated time for completion is 6 weeks from project start to project end. **Assumptions:** 1. Vulnerability scanning will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. 2. Vulnerability scanning will be performed in a non-production environment that minimizes disruption to business services 3. DIR Customer will identify a “trusted agent” responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 4. DIR Customer will facilitate remote access to the non-production application within three (3) business days of the project start date 5. DIR Customer will provide required credentials to perform testing within three (3) business days of the project start date 6. DIR Customer Price provided is on a per application basis (one application) 7. DIR Customer will be responsible for remediation of findings 8. Deloitte will test up to one hundred (100) dynamic web pages per web application 9. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within seven (7) business days of submission, and issuance of final deliverable by Deloitte) 10. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 149,100.00	Project cost	10.00%	$135,196.43

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Threat Detection and Security Monitoring - Vulnerability scanning and management : Web Application Scanning (Medium)	**Service description:** The objective of this service it to identify potential vulnerabilities which might be used by attackers to compromise web-based applications, the data within the applications, and / or supporting infrastructure. As part of our service offering, we will perform automated vulnerability tests and use manual testing techniques along with our proprietary knowledgebase of application attack profiles and web server vulnerabilities to test the application servers for possible exposures to vulnerabilities. We will map the confirmed vulnerabilities to the top ten (10) vulnerability categories of Open Web Application Security Project (OWASP). **Service activities:** 1. Define scope and plan, identify "trusted agent", gather list in-scope web applications and supporting infrastructure, agree upon logistics and scanning rules 2. Confirmation of connectivity, tools operation, overview of in-scope applications and supporting infrastructure, and gather required credentials and access to perform scanning 3. Perform analysis of the application security controls, including black-box and grey-box testing, perform scans 4. Manual assessment of results, including false-positive and false-negative testing and rationalization of weaknesses noted 5. Confirm observations with trusted agent and stakeholders, and creation of vulnerability assessment report which includes control gaps / weaknesses and corrective action plans **Service duration:** The estimated time for completion is 4 weeks from project start to project end. **Assumptions:** 1. Vulnerability scanning will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. 2. Vulnerability scanning will be performed in a non-production environment that minimizes disruption to business services 3. DIR customer will identify a “trusted agent” responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 4. DIR customer will facilitate remote access to the non-production application within three (3) business days of the project start date 5. DIR customer will provide required credentials to perform testing within three (3) business days of the project start date 6. DIR Customer Price provided is on a per application basis (one application) 7. DIR Customer will be responsible for remediation of findings 8. Deloitte will test up to seventy (70) dynamic web pages per web application 9. Deliverable acceptance process includes one review cycle (1 draft submitted for review, written feedback provided to Deloitte within five (5) business days of submission, and issuance of final deliverable by Deloitte) 10. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 99,400.00	Project cost	10.00%	$90,130.95

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Threat Detection and Security Monitoring - Vulnerability scanning and management : Web Application Scanning (Simple)	**Service description:** The objective of this service it to identify potential vulnerabilities which might be used by attackers to compromise web-based applications, the data within the applications, and / or supporting infrastructure. As part of our service offering, we will perform automated vulnerability tests and use manual testing techniques along with our proprietary knowledgebase of application attack profiles and web server vulnerabilities to test the application servers for possible exposures to vulnerabilities. We will map the confirmed vulnerabilities to the top ten (10) vulnerability categories of Open Web Application Security Project (OWASP). **Service activities:** 1. Refine scope and plan, identify "trusted agent", gather list in-scope web applications and supporting infrastructure, agree upon logistics and scanning rules 2. Confirmation of connectivity, tools operation, overview of in-scope applications and supporting infrastructure, and gather required credentials and access to perform scanning 3. Perform analysis of the application security controls, including black-box and grey-box testing, perform scans 4. Manual assessment of results, including false-positive and false-negative testing and rationalization of weaknesses noted 5. Confirm observations with trusted agent and stakeholders, and creation of vulnerability assessment report which includes control gaps / weaknesses and corrective action plans **Service duration:** The estimated time for completion is 3 weeks from project start to project end. **Assumptions:** 1. Vulnerability scanning will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. 2. Vulnerability scanning will be performed in a non-production environment that minimizes disruption to business services 3. DIR Customer will identify a “trusted agent” responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 4. DIR Customer will facilitate remote access to the non-production application within three (3) business days of the project start date 5. DIR Customer will provide required credentials to perform testing within three (3) business days of the project start date 6. DIR Customer Price provided is on a per application basis (one application) 7. Deloitte will test up to thirty five (35) dynamic web pages per web application 8. DIR Customer will be responsible for remediation of findings 9. Deliverable acceptance process includes one review cycle (1 draft submitted for review, written feedback provided to Deloitte within three (3) business days of submission, and issuance of final deliverable by Deloitte) 10. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 49,700.00	Project cost	10.00%	$45,065.48

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Threat Detection and Security Monitoring - Vulnerability scanning and management : Web Application Scanning (Very Large)	**Service description:** The objective of this service it to identify potential vulnerabilities which might be used by attackers to compromise web-based applications, the data within the applications, and / or supporting infrastructure. As part of our service offering, we will perform automated vulnerability tests and use manual testing techniques along with our proprietary knowledgebase of application attack profiles and web server vulnerabilities to test the application servers for possible exposures to vulnerabilities. We will map the confirmed vulnerabilities to the top ten (10) vulnerability categories of Open Web Application Security Project (OWASP). **Service activities:** 1. Refine scope and plan, identify "trusted agent", gather list in-scope web applications and supporting infrastructure, agree upon logistics and scanning rules 2. Confirmation of connectivity, tools operation, overview of in-scope applications and supporting infrastructure, and gather required credentials and access to perform scanning 3. Perform analysis of the application security controls, including black-box and grey-box testing, perform scans 4. Manual assessment of results, including false-positive and false-negative testing and rationalization of weaknesses noted 5. Confirm observations with trusted agent and stakeholders, and creation of vulnerability assessment report which includes control gaps / weaknesses and corrective action plans **Service duration:** The estimated time for completion is 12 weeks from project start to project end. **Assumptions** 1. Vulnerability scanning will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. 2. Vulnerability scanning will be performed in a non-production environment that minimizes disruption to business services 3. DIR Customer will identify a “trusted agent” responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 4. DIR Customer will facilitate remote access to the non-production application within three (3) business days of the project start date 5. DIR Customer will provide required credentials to perform testing within three (3) business days of the project start date 6. DIR Customer Price provided is on a per application basis (one application) 7. DIR Customer will be responsible for remediation of findings 8. Deloitte will test up to one hundred seventy five (175) dynamic web pages per web application 9. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within seven (7) business days of submission, and issuance of final deliverable by Deloitte) 10. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 298,300.00	Project cost	10.00%	$270,483.53

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Training and Awareness - Cybersecurity program evaluation: Enterprise Fraud Program Assessment (Large)	**Service description:** The purpose of this service is to review the agency fraud program to determine if the appropriate skill sets, processes, organization integration, and technologies are in place to detect/manage potential emerging fraud issues. This assessment includes a review of the agency's internet application transaction and web server logs using Deloitte & Touche LLP's ("Deloitte") current cyber intelligence feeds to identify potential fraudulent transactions. **Service activities:** Deloitte performs an assessment of the current state of a mid-sized sized agency (1,000-9,999 employees), up to one (1) Terabyte (TB) of audit log files using five (5) potential fraud detection rule sets **Service duration:** The estimated time for completion is 8 weeks from project start to project end. **Assumptions:** 1. Enterprise fraud program assessment will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems ("servers, workstations and desktops) within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within seven (7) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 198,800.00	Project cost	10.00%	$180,261.90

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Training and Awareness - Cybersecurity program evaluation: Enterprise Fraud Program Assessment (Medium)	**Service description:** The purpose of this service is to review the agency fraud program to determine if the appropriate skill sets, processes, organization integration, and technologies are in place to detect/manage potential emerging fraud issues. This assessment includes a review of the agency's internet application transaction and web server logs using Deloitte & Touche LLP's ("Deloitte") current cyber intelligence feeds to identify potential fraudulent transactions. **Service activities:** Deloitte performs an assessment of the current state of a small sized agency (100-999 employees), up to five hundred (500) Gigabyte (GB) of audit log files using five (5) potential fraud detection rule sets. **Service duration:** The estimated time for completion is 6 weeks from project start to project end. **Assumptions:** 1. Enterprise fraud program assessment will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems ("servers, workstations and desktops) within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within five (5) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 149,100.00	Project cost	10.00%	$135,196.43

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Training and Awareness - Cybersecurity program evaluation: Enterprise Fraud Program Assessment (Simple)	**Service description:** The purpose of this service is to review the agency fraud program to determine if the appropriate skill sets, processes, organization integration, and technologies are in place to detect/manage potential emerging fraud issues. This assessment includes a review of the agency's internet application transaction and web server logs using Deloitte & Touche LLP's ("Deloitte") current cyber intelligence feeds to identify potential fraudulent transactions. **Service activities:** Deloitte performs an assessment of the current state of a very-small sized agency (1-99 employees), up to two hundred and fifty (250) Gigabyte (GB) of audit log files using three (3) potential fraud detection rule sets. **Service duration:** The estimated time for completion is 3 weeks from project start to project end. **Assumptions:** 1. Enterprise fraud program assessment will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within three (3) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 74,600.00	Project cost	10.00%	$67,643.55

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Training and Awareness - Cybersecurity program evaluation: Enterprise Fraud Program Assessment (Very Large)	**Service description:** The purpose of this service is to review the agency fraud program to determine if the appropriate skill sets, processes, organization integration, and technologies are in place to detect/manage potential emerging fraud issues. This assessment includes a review of the agency's internet application transaction and web server logs using Deloitte's current cyber intelligence feeds to identify potential fraudulent transactions. **Service activities:** Deloitte assess the current state of a large sized agency (1,000-9,999 employees), up to two (2) Terabyte (TB) of audit log files using five (5) potential fraud detection rule sets **Service duration:** The estimated time for completion is 12 weeks from project start to project end. **Assumptions:** 1. Enterprise fraud program assessment will be performed remotely from Deloitte & Touche LLP ("Deloitte") Cyber Security Center(s) located in the United States 2. DIR Customer will identify a "trusted agent" responsible for coordinating all on-site activities at the customer site and working with Deloitte point of contact 3. DIR Customer will facilitate remote access to the in-scope systems ("servers, workstations and desktops) within three (3) business days of the project start date 4. DIR Customer will provide required credentials to perform analysis within three (3) business days of the project start date 5. DIR Customer will be responsible for remediation of findings 6. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within seven (7) business days of submission, and issuance of final deliverable by Deloitte). 7. DIR Customer Price was derived assuming that the activities for this services will be performed remotely from Deloitte Cyber Security Center(s) located in the United States. However, if required this service may also be available to DIR Customer through a delivery model that is on-site at DIR Customer location. Deloitte welcomes the opportunity to discuss the DIR Customer Price for this service performed on-site at DIR Customer location.	$ 298,300.00	Project cost	10.00%	$270,483.53

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Training and Awareness - Cybersecurity risk assessment and management: Focused Assessment	**Service description:** Deloitte & Touche LLP ("Deloitte") performs an information security risk assessment (IRSA) following Deloitte's methodology which is based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Revision 1, the Guide for Conducting Risk Assessments. Through an ISRA, Deloitte identifies gaps and instances of non-compliance with applicable regulatory requirements, State and Federal laws, as well as local policies. Deloitte leverages the Integrated Risk and Controls Framework as the baseline for the assessment. The framework covers numerous accepted industry standards, including: NIST Special Publications, International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001, ISO/IEC 27002, Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH), Health Information Trust Alliance (HITRUST), and Payment Card Industry (PCI) Data Security Standard (DSS). As result of the ISRA, Deloitte assists State agencies on the risk ranking of identified gaps and development of corrective action plans. For a focused ISRA, the State agency selects one regulation or industry standard to be assessed against. This is especially useful for regulatory requirements such as HIPAA or Internal Revenue Service (IRS) Publication 1075. A focused assessment differs from a foundational assessment with a focus on specific federal or state regulatory requirements or standards; or for a non-technical controls based assessment of an application. **Service activities:** 1. Scope and plan: Confirm project scope, conducts kick-off with stakeholders and sponsors, confirms deliverable templates, and schedules workshops 2. Understand requirements: Refine regulations and industry standards to be in-scope. Optionally, select an application for a non-technical controls assessment. 3. Conduct ISRA: Using the customized framework, Deloitte performs an assessment based on workshops, interviews, and review of applicable documentation 4. Rationalize and validate gaps: Deloitte discusses preliminary gaps with stakeholders, updates results based on validation workshops, and finally risk-ranks gaps and develops corrective action plans for validated gaps 5. Reporting: Develop ISRA report, including description of gaps, risk per gap, and corrective action plans. ISRA reports also include an executive summary to showcase results in themes for consumption by executives **Service duration:** The estimated time for completion is 4 weeks from project start to project end. **Assumptions:** Basic ISRAs provide a detailed view of the maturity and level of compliance of an agency with selected regulatory requirements or industry standards. The following assumptions were considered during the refinement of DIR customer pricing: 1. Up to two (2) regulation or industry standard to be selected for the assessment; or up to one (2) applications 2. Responses to Deloitte's assessment questionnaire and request for information required for the assessment will be responded to by the State within 3 business days of the request 3. Steps 1, 2, 4, and 5 from service activities listed under Detailed Service Description column will be conducted remotely 4. If required, up to six (6) workshops to be conducted onsite (Step 3). ISRA workshops and interviews will occur within two continuous weeks (Step 3) 5. Deliverable acceptance process includes one review cycle (1 draft submitted for review, written feedback provided to Deloitte within two (2) business days of submission, and issuance of final deliverable by Deloitte)	$ 99,400.00	Project cost	10.00%	$90,130.95

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Training and Awareness - Cybersecurity risk assessment and management: Foundational Assessment	**Service description:** Deloitte & Touche LLP ("Deloitte") performs an information security risk assessment (IRSA) following Deloitte's methodology which is based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Revision 1, the Guide for Conducting Risk Assessments. Through an ISRA, Deloitte identifies gaps and instances of non-compliance with applicable regulatory requirements, State and Federal laws, as well as local policies. Deloitte leverages the Integrated Risk and Controls Framework as the baseline for the assessment. The framework covers numerous accepted industry standards, including: NIST Special Publications, International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001, ISO/IEC 27002, Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH), Health Information Trust Alliance (HITRUST), and Payment Card Industry (PCI) Data Security Standard (DSS). As result of the ISRA, Deloitte assists State agencies on the risk ranking of identified gaps and development of corrective action plans. **Service activities:** 1. Scope and plan: Confirm project scope, conducts kick-off with stakeholders and sponsors, confirms deliverable templates, and schedules workshops 2. Understand requirements: Refine regulations and industry standards to be in-scope 3. Conduct ISRA: Using the customized framework, Deloitte performs an assessment based on responses to Deloitte prepared assessment questionnaire and review of applicable documentation 4. Rationalize and validate gaps: Deloitte discusses preliminary gaps with stakeholders, updates results based on validation workshops, and finally risk-ranks gaps and develops corrective action plans for validated gaps 5. Reporting: Develop ISRA report, including description of gaps, risk per gap, and corrective action plans. ISRA reports also include an executive summary to showcase results in themes for consumption by executives **Service duration:** The estimated time for completion is 3 weeks from project start to project end. **Assumptions:** Foundational ISRAs provide a high level overview of the current information security posture of the assessed agency. The following assumptions were considered during the refinement of DIR customer pricing: 1. The scope of this assessment includes assessment of up to fifty (50) security requirements from up to five (5) security domains from up to two (2) industry standards. The assessment will be performed primarily by evaluation DIR Customer's responses to a Deloitte's customized questionnaire prepared for the selected security requirements. 2. Steps 1, 2, 4, and 5 from service activities listed under Detailed Service Description column will be conducted remotely 3. Responses to Deloitte's assessment questionnaire and request for information required for the assessment will be responded to by the State within three (3) business days of the request 4. If required, up to three (3) workshops to be conducted onsite (Step 3). These workshops and interviews will occur within one (1) week. 5. Deliverable acceptance process includes one (1) review cycle (1 draft submitted for review, written feedback provided to Deloitte within two (2) business days of submission, and issuance of final deliverable by Deloitte)	$ 49,700.00	Project cost	10.00%	$45,065.48

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Training and Awareness - Cybersecurity training software and services	Services provided using Knowbe4 platform. **Service description:** The objective of this service is to educate employees and Key stakeholders leveraging software and services. **Service activities:** 1. Define scope of project 2. Work with Human Resources to develop communication plan 3. Integrate Security Awareness platform into existing processes 4. Decide whether platform will be used for Onboarding and Ongoing training requirements 5. Integrate users in Training platform 6. Lunch Security Awareness Training using the platform 7. Track completion results 8. Work with Client to decide on next steps **Service duration:** The estimated time for completion is four (4) weeks from project start to project end. (time to vary based on the deployment size) **Assumptions:** n/a	$ 20,200.00	Project Cost	10.00%	$18,316.35

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Training and Awareness - Incidence response training: Cyber Drill	**Service description:** Our exercises immerse participants in a simulated and interactive cyber-attack scenario, allowing organizations to test their response reflexes, identify capability gaps, and train on and develop advanced preparedness techniques. Engagements are led by specialists with deep knowledge of applicable regulations, law enforcement and cyber intelligence, informed by Deloitte & Touche LLP's ("Deloitte") broad experience across many industry sectors. Incorporating methods from military and academic research, our approach has been refined through engagements with multi-national companies, government entities, regulatory bodies, and industry groups. The exercises utilize gamification techniques that appeal to natural human tendencies, and leverage a toolkit of accelerators, such as a repository of scenarios and inject templates, to enhance and expedite exercise development and delivery. A Cyber Drill is a facilitated exercise where participants are guided through their organization's planned response to a straightforward cyber incident. Benefits of this service include: 1. Increases participant awareness of cyber threats applicable to the organization 2. Introduces the organization's cyber incident response processes and capabilities to participants 3. Assesses participant understanding of the organization's cyber incident response processes and capabilities 4. Provides an effective platform to validate cyber incident response plan and procedure design **Service activities:** 1. Define cyber drill exercise ("exercise") goals and high-level design attributes 2. Develop exercise design (simulating a straightforward cyber incident) and delivery plan – with assistance from one (1) – two (2) client 'trusted agents' 3. Support DIR Customer's efforts to coordinate exercise logistics (defining participant roster, selecting venue, validating technology, conducting education session to set expectations for participants prior to exercise, etc.) 4. Create exercise materials 5. Conduct dry-run and refine exercise materials – with assistance from 1-2 client 'trusted agents' 6. Conduct exercise 7. Develop exercise summary document **Service duration:** The estimated time for completion is 6 weeks from project start to project end. **Assumptions:** 1. The preparation time required prior to cyber drill exercise ("exercise") delivery is approximately four (4) weeks 2. The total number of hours required from client sponsors / 'trusted agents' to support exercise design activities is six (6) – eight (8) hours 3. The total exercise duration is no more than three (3) hours, inclusive of a pre-brief, simulation, and debrief 4. The total number of exercise players is no more than eight (8) people, all in the same physical location 5. Exercise injects are delivered via a paper-based inject pack, client actor, on-screen presentation and/or pre-recorded audio 6. Upfront interviews to support exercise design are primarily conducted on-site; creation of materials build is primarily completed off-site 7. The exercise does not include any system scanning or testing activities (e.g., penetration testing, vulnerability scanning)	$ 149,100.00	Project cost	10.00%	$135,196.43

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Training and Awareness - Incidence response training: Cyber Tabletop	**Service description:** Our exercises immerse participants in a simulated and interactive cyber-attack scenario, allowing organizations to test their response reflexes, identify capability gaps, and train on and develop advanced preparedness techniques. Engagements are led by specialists with deep knowledge of applicable regulations, law enforcement and cyber intelligence, informed by Deloitte & Touche LLP's ("Deloitte") broad experience across many industry sectors. Incorporating methods from military and academic research, our approach has been refined through engagements with multi-national companies, government entities, regulatory bodies, and industry groups. The exercises utilize gamification techniques that appeal to natural human tendencies, and leverage a toolkit of accelerators, such as a repository of scenarios and inject templates, to enhance and expedite war game development and delivery. A Cyber Tabletop is a facilitated exercise where players practice response, with facilitator guidance, to a semi-complex cyber incident. Benefits of this service include: 1. Involves a larger set of likely cyber incident responders (to address a broader set of threat actors and attack-types) 2. Assesses participant ability to deploy the organization's cyber incident response processes and capabilities 3. Provides an effective platform to validate cyber incident response communication and coordination capabilities 4. Familiarizes participants with simulation-type exercises **Service activities:** 1. Define cyber tabletop exercise ("exercise") goals and high-level design attributes 2. Develop full exercise design (simulating a semi-complex cyber incident) and delivery plan – with assistance from 2-4 client 'trusted agents' 3. Support client efforts to coordinate exercise logistics (defining participant roster, selecting venue, validating technology, conducting education session to set expectations for participants prior to exercise, etc.) 4. Create exercise materials 5. Conduct dry-run and refine exercise materials – with assistance from 2-4 client 'trusted agents' 6. Conduct exercise 7. Develop abbreviated After Action Report **Service duration:** The estimated time for completion is 8 weeks from project start to project end. **Assumptions:** 1. The preparation time required prior to cyber tabletop exercise ("exercise") delivery is approximately six (6) weeks 2. The total number of hours required from client sponsors / 'trusted agents' to support exercise design activities is twenty (20) – thirty (30) hours 3. The total exercise duration is no more than three (3) hours, inclusive of a pre-brief, simulation, and debrief 4. The total number of exercise players is no more than fifteen (15) people, all in the same physical location 5. Exercise injects are delivered via a paper-based inject pack, client actor, on-screen presentation and/or pre-recorded audio 6. Upfront interviews to support exercise design are primarily conducted on-site; creation of materials build is primarily completed off-site 7. The exercise does not include any system scanning or testing activities (e.g., penetration testing, vulnerability scanning)	$ 198,800.00	Project cost	10.00%	$180,261.90

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Training and Awareness - Incidence response training: Cyber Wargame	**Service description:** Our exercises immerse participants in a simulated and interactive cyber-attack scenario, allowing organizations to test their response reflexes, identify capability gaps, and train on and develop advanced preparedness techniques. Engagements are led by specialists with deep knowledge of applicable regulations, law enforcement and cyber intelligence, informed by Deloitte & Touche LLP's ("Deloitte") broad experience across many industry sectors. Incorporating methods from military and academic research, our approach has been refined through engagements with multi-national companies, government entities, regulatory bodies, and industry groups. The exercises utilize gamification techniques that appeal to natural human tendencies, and leverage a toolkit of accelerators, such as a repository of scenarios and inject templates, to enhance and expedite war game development and delivery. 1. A Cyber Wargame is a facilitated exercise where players' abilities to respond to a cyber incident are stress tested against a complex cyber incident. Benefits of this service include: 2. Assesses participants' ability to deploy the organization's cyber incident response processes and capabilities to address a complex cyber-attack 3. Stress-tests the assignment of resources/ prioritization of response activities to address a complex cyber-attack 4. Provides an effective platform to validate cyber incident response command and control capabilities **Service activities:** 1. Define cyber wargame exercise ("exercise") goals and high-level design attributes 2. Develop full exercise design (simulating a complex cyber incident) and delivery plan – with assistance from three (3) – six (6) client 'trusted agents' 3. Support client efforts to coordinate exercise logistics (defining participant roster, selecting venue, validating technology, conducting education session to set expectations for participants prior to exercise, etc.) 4. Create exercise materials 5. Conduct dry-run and refine exercise materials – with assistance from 3-6 client 'trusted agents' 6. Conduct exercise 7. Develop After Action Report **Service duration:** The estimated time for completion is 12 weeks from project start to project end. **Assumptions:** 1. The preparation time required prior to exercise delivery is approximately 9 weeks 2. The total number of hours required from client sponsors / 'trusted agents' to support exercise design activities is thirty (30) plus hours 3. The total exercise duration is no more than three (3) hours, inclusive of a pre-brief, simulation, and debrief 4. The total number of exercise players is no more than thirty (30) people, all in the same physical location 5. Exercise injects are delivered via a paper-based inject pack, client actor, on-screen presentation and/or pre-recorded audio 6. Upfront interviews to support exercise design are primarily conducted on-site; creation of materials build is primarily completed off-site 7. The exercise does not include any system scanning or testing activities (e.g., penetration testing, vulnerability scanning)	$ 298,300.00	Project cost	10.00%	$270,483.53

SERVICE NAME	SERVICE DESCRIPTION	List COST Per Unit	Unit of Issue	Discount % off	DIR Customer Price Each
Training and Awareness - Provide cybersecurity awareness training to prevent phishing and other attacks	**Service description:** The objective of this service is to educate employees and Key stakeholders on how to recognize and react to potential malicious emails. Cybersecurity awareness training - Phishing Simulation. **Service activities:** 1. Define scope of project 2. Develop and send communication plan 3. Send Baseline Phishing campaign 4. Decide whether to announce program 5. Launch Program 6. Review results and next step 7. Knowledge transfer **Service duration:** The estimated time for completion is four (4) weeks from project start to project end. (time to vary based on the deployment size) **Assumptions:** n/a	$ 17,800.00	Project Cost	10.00%	$16,140.15